Riscos e vulnerabilidades dos equipamentos IoT em unidades de saúde

Mestrado de Cibersegurança e Informática Forense

João Tomé de Carvalho Gomes

Leiria, setembro de 2019

Riscos e vulnerabilidades dos equipamentos IoT em unidades de saúde

Mestrado de Cibersegurança e Informática Forense

João Tomé de Carvalho Gomes

Dissertação de Projeto realizado sob a orientação dos Professor Doutor António Manuel Jesus Pereira e do Professor Doutor Luis Alexandre Lopes Frazão.

Leiria, setembro de 2019

Originalidade e Direitos de Autor

A presente dissertação de projeto é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Reproduções parciais deste documento serão autorizadas na condição de que seja mencionado o Autor e feita referência ao ciclo de estudos no âmbito do qual o mesmo foi realizado, a saber, Curso de Mestrado em Cibersegurança e Informática Forense, no ano letivo 2018/2019, da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, Portugal, e, bem assim, à data das provas públicas que visaram a avaliação destes trabalhos.

Dedicatória

À minha família, em especial à minha esposa Ana Rita pela compreensão na realização deste trabalho e à minha filha Flor que me deu ânimo e força para concluir este trabalho numa fase muito complicada da minha vida.

A ti mãe, que ficaste tão contente no dia em que te disse que ia voltar a estudar, certamente que ficarás orgulhosa por ter concluído este curso.

Agradecimentos

Quero expressar os meus sinceros agradecimentos a todas as pessoas que direta ou indiretamente, contribuíram para a realização deste trabalho.

De enaltecer o incentivo e o apoio prestado ao longo deste processo de dissertação, ao Professor António Pereira e ao Professor Luis Frazão, sem os quais seria impossível concluí-lo com sucesso.

Agradeço também a todos os professores que fizeram parte do meu percurso académico no IPL, por tudo o que me transmitiram e pelo enriquecimento que me proporcionaram ao longo da minha formação académica.

Agradeço ainda à Escola Superior de Tecnologia e Gestão de Leiria, pelos meios e condições que colocaram à minha disposição para a realização deste mestrado.

De salientar que este trabalho não seria possível sem o know-how que ganho diariamente na unidade de saúde onde trabalho, pelo que agradeço à minha entidade patronal e a todos os colaboradores com quem partilho experiências com equipamentos IoT diariamente.

Por fim, gostaria de agradecer a toda a minha família, amigos e a todas as pessoas que são especialmente chegadas, por todo o apoio prestado, que de uma forma ou de outra, facilitaram o caminho a alcançar esta etapa.

Resumo

A internet das coisas, ou em inglês “Internet of Things”, ganhou o nome “IoT” e este tipo de equipamentos enraizou-se muito rapidamente no nosso quotidiano. Os IoT têm evoluído rapidamente e estão cada vez mais presentes no nosso quotidiano. São pequenos equipamentos dotados de uma ampla variedade de sistemas de monitorização e de dispositivos de comunicações com a particularidade de se ligarem à internet para recolherem dados para transmitir a informação de diversos sensores para a rede.

A presente dissertação tem como objetivo principal a criação de um manual de regras de boas práticas para implementação de equipamentos IoT em unidades de saúde, com especial enlace na confidencialidade, na autenticidade, na integridade e na disponibilidade da informação, sempre a pensar na segurança dos dados das instituições. A decisão por se elaborar este manual é baseada na inexistência deste tipo de documentação para esta área tão sensível que é a saúde.

Para elaborar este conjunto de boas práticas foi necessário abordar os tipos de comunicação, perceber qual a motivação para comprometer a segurança, elencar os tipos de ataques mais comuns assim como os tipos de ameaça. Foram caracterizados alguns dos equipamentos presentes nas unidades de saúde de forma a perceber quais os riscos e as vulnerabilidades a que estes estão sujeitos.

Com este manual de boas práticas para implementação de equipamentos IoT em unidades de saúde vai ser possível dotar as organizações de um guia com regras para implementação que poderão adotar ou que poderão seguir para implementar IoT na sua infraestrutura de rede.

As organizações ao seguir este conjunto de boas práticas irão ficar dotadas de uma melhor cultura ao nível de segurança, e certamente tomarão consciência das fragilidades que têm na rede, uma vez que esta dissertação ajudará a conhecer alguns dos riscos e das vulnerabilidades que os equipamentos detêm.

Palavras-chave: IoT, saúde, riscos, vulnerabilidades, boas práticas

Abstract

The internet of things, or "Internet of Things", has earned the name "IoT" and this kind of equipment has taken root very quickly in our daily lives. IoTs have evolved rapidly and are increasingly present in our daily lives. They are small devices equipped with a wide variety of monitoring systems and communication devices with the particularity of connecting to the internet to collect data to transmit information from various sensors to the network.

This dissertation has as main objective the creation of a manual of best practice rules for the implementation of IoT equipment in health facilities, with special emphasis on confidentiality, authenticity, integrity and availability of information, always thinking about the security of data from the institutions. The decision to draw up this manual is based on the lack of such documentation for this health sensitive area.

To elaborate this set of good practices it was necessary to address the types of communication, understand the motivation to compromise security, list the most common types of attacks as well as the types of threats. Some of the equipment present in health facilities were characterized in order to understand which risks and vulnerabilities they are subject to.

This good practice manual for deploying IoT equipment in healthcare facilities will provide organizations with a guide to implementation rules that they can adopt or follow to implement IoT in their network infrastructure.

Organizations following this set of good practices will gain a better culture of security, and will certainly be aware of the weaknesses they have in the network, as this dissertation will help to know some of the risks and vulnerabilities that equipment holds.

Keywords: IoT, health, risks, vulnerabilities, good practices

Índice

Lista de Figuras

Lista de tabelas

Lista de siglas e acrónimos

2FA	Two Factor Authetication / Dois fatores de autenticação
API	Application Programming Interface
CoAP	Constrained Application Protocol
CNC	Centro Nacional de Cibersegurança
CSRF	Cross-site request forgery
CVE	Common Vulnerabilities and Exposures
DICOM	Digital Imaging and Communications in Medicine
DoS	Denial Of Service
ECG	Eletrocardiograma
ESTG	Escola Superior de Tecnologia e Gestão
HL7	Health Level Seven
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IDS	Intrusion detection system
IoT	Internet of things
IPS	Intrusion prevention system
IPv6	Internet Protocol v6
LAN	Local Area Network
MAN	Metropolitan Area Network
MQTT	Message Queue Telemetry Transport
NFC	Near Field Communication
PACS	Picture Archiving and Communication System
PAN	Personal Area Network
QGBT	Quadro geral de baixa tensão
REST	Representational State Transfer
RFID	Radio Frequency Identification
RGPD	Regime Geral de Proteção de Dados
SD	Secure Digital Card
SIEM	Security Information and Event Management
SMS	Short Message Service

SQLi	Structured Query Language *Injection*
SSID	Service Set Identifier
TI	Tecnologias de Informação
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
XSS	Cross-site scripting

1. Introdução

Nos últimos anos o sector da saúde rendeu-se com grande entusiasmo à Internet das Coisas (IoT-Internet of Things). Estes equipamentos inteligentes possuem um enorme potencial ao proporcionarem um melhor diagnóstico, um melhor tratamento e consequentemente fornecem ajuda preciosa a salvar vidas uma vez que recolhem e analisam dados médicos que antes estavam inacessíveis. Permitem assim aos profissionais da saúde prestar tratamentos essenciais e personalizados de forma mais rápida e direta, com uma monitorização ativa e permanente.

Esta proliferação de tecnologia tem implicações preocupantes no que toca à integridade de dados sensíveis sobre os pacientes e ao funcionamento contínuo e sem falhas dos sistemas. Os equipamentos IoT da saúde precisam de ser capazes de proteger todos os dados que recolhem, que transmitem e que guardam, mantendo-os a salvo de indivíduos que pretendam intercetá-los. Isto significa que se não forem desenhados e construídos tendo como principal premissa a sua segurança, é muito provável que em breve venham a tornar-se vulneráveis e a comprometer a saúde e segurança do doente.

Num mundo cada vez mais digital, as equipas de sistemas de informação das mais variadas instituições ou organizações, necessitam de ser mais observadoras e acompanhar de perto as mudanças tecnológicas que possam potencialmente afetar o negócio em que estão inseridos.

Conforme a IoT se prolifera pela sociedade recolhendo cada vez mais dados a partir de objetos, máquinas e pessoas, as organizações enfrentam diariamente novas oportunidades, variadíssimos riscos e desafios preocupantes ao nível de segurança com que deverão saber lidar e estar atentos.

Nas unidades de saúde o uso destas tecnologias têm acompanhado a tendência global, e a proliferação de equipamentos também se tem sentido e enraizando nestas organizações, no entanto traz consigo variadíssimos riscos e vulnerabilidades.

A Internet das Coisas ou os IoT podem de facto ajudar a escrever uma nova página na vida dos utentes e na forma como ajudam os sistemas de saúde a proporcionar melhor qualidade de vida, mas podem também ser uma porta aberta aos cibercriminosos ou a pessoas mal

intencionadas, cuja única motivação é o lucro financeiro, mesmo que para isso possam causar indisponibilidade ou até a morte do doente.

Em ambientes hospitalares ou unidades de saúde é necessário uma monitorização constante dos ativos que se ligam á rede, uma vez que se trata de ambientes críticos e sensíveis, onde pequenos erros ou pequenos problemas podem resultar numa fatalidade.

Assim, os equipamentos de saúde ligados em rede tornam-se uma mais valia ás equipas multidisciplinares no terreno, ajudando-os a tomar uma melhor decisão ou a emitir alertas aquando um determinado evento.

O procedimento adotado atualmente em diversas unidades de saúde para a monitorização de determinadas rotinas ainda é realizada de forma manual, em horários estipulados procedendo na maioria dos casos a um eventual registo em papel propício a erros, no entanto o paradigma está a mudar e em algumas unidades de saúde estes procedimentos já são automáticos, utilizando sondas e sensores que possibilitam a recolha de informação com maior rigor e eficácia em horários estipulados e cíclicos.

O IoT tem se desenvolvido cada vez mais e trazido consigo muitas melhorias indispensáveis ao nosso dia-a-dia. Hoje é notário que graças a estes equipamentos pequenos erros que aconteciam no passado já não ocorrem.

Ao mesmo tempo que a IoT proporciona benefícios valiosos nas instituições, os riscos de exposição a diversas ameaças de segurança e de privacidade aumentam exponencialmente, na sua maioria estas ameaças são novas e particulares desta tecnologia.

Com o aumento exponencial de equipamentos ligados em rede, os equipamentos IoT ficam expostos a várias vulnerabilidades na comunicação, apresentando uma infraestrutura variável e na sua maioria estes equipamentos possuem recursos limitados, com capacidade de armazenamento limitado e baixa energia.

Neste trabalho aborda-se a temática atual da falta de segurança dos equipamentos IoT, elencando os principais riscos e vulnerabilidades que alguns equipamentos presentes em unidades de saúde estão sujeitos, elaborando uma lista de boas práticas para implementação destes equipamentos num ecossistema sensível como é um hospital, um centro de saúde, uma clínica, uma farmácia ou um laboratório.

1.1. Objetivos e contribuições

Focando a questão da segurança e dos diversos ataques que tem ocorrido aos múltiplos equipamentos que são ligados diariamente ás redes de unidades de saúde, os principais objetivos desta dissertação são a identificação e a definição de procedimentos de boas práticas e mecanismos de segurança para equipamentos de saúde.

Após analisar o estado da arte e entender os tipos de comunicação dos equipamentos IoT, foram verificados quais os tipos de ameaça e os ataques mais comuns a que estes equipamentos estão propensos. Foram também elencados os principais tipos de comunicação, assim como os protocolos mais utilizados e as respetivas normas que existem para este tipo de equipamentos.

A primeira contribuição deste trabalho consiste na caracterização dos principais equipamentos utilizados em unidades de saúde, em particular os equipamentos IoT que estão ligados á rede e que produzem informação, alguma de teor sensível ou confidencial.

A segunda contribuição, foca-se na identificação dos principais riscos a que os equipamentos IoT estão sujeitos em unidades de saúde, elencando os riscos mais conhecidos que advém da utilização destes equipamentos.

A terceira contribuição deste trabalho centra-se nas vulnerabilidades mais comuns que podem ser encontradas em equipamentos IoT neste tipo de instituições com principal enlace na segurança do doente e na proteção e salvaguarda dos dados que são gerados diariamente.

Das contribuições anteriores resultou a definição de procedimentos e de regras de boas práticas para implementação destes equipamentos em unidades ou instituições de saúde.

No último capítulo, resumem-se as conclusões tiradas e perspetiva-se algumas medidas preventivas assim como o trabalho futuro que poderá ser desenvolvido.

1.2. Estrutura

Na prossecução dos objetivos e contribuições definidos anteriormente, o presente trabalho começa por apresentar no capítulo 2, o estado da arte do IoT, seguindo-se os tipos de comunicação inerentes ao seu funcionamento. São abordadas também as motivações para comprometer a segurança a equipamentos em unidades de saúde, assim como os diversos

ataques de segurança conhecidos e foram estudados quais as principais ameaças inerentes a este tipo de equipamentos.

Na sequência do estado da arte, no capítulo 3 é apresentada uma caracterização dos principais equipamentos utilizados em unidades de saúde que podem comprometer a segurança e a integridade da informação neste ambiente.

No capítulo 3 são também analisados os principais riscos dos equipamentos IoT, onde é abordado o risco da recolha massiva de dados, da confidencialidade e fiabilidade, do controlo de acessos, dos middleware inseguros, das redes programáveis, dos ataques baseados em botnets, das falhas de energia, do big data, do malware, da interoperabilidade, da falsificação e dos pontos de acesso.

Neste capítulo são também apresentadas as principais vulnerabilidades dos equipamentos IoT, nomeadamente relativamente ao acesso remoto, aos testes de penetração, aos ataques de bruteforce, as senhas fracas, os backdoors, os firmware inseguro, e a ausência de adoção de padrões.

No capítulo 4 são apresentadas as regras para implementação de equipamentos IoT em unidades de saúde, evidenciando as boas práticas para tornar a rede mais segura, assim como dotar os profissionais que trabalham com os equipamentos no seu dia-a-dia de know-how diferenciado de forma a tornar o ecossistema onde se inserem isento de problemas que podem comprometer a continuidade de negócio.

A conclusão é efetuada no capítulo 5 onde são apresentadas as conclusões relativas ao trabalho realizado e dadas algumas indicações para o trabalho futuro.

2. Estado da Arte

O rápido avanço tecnológico que se tem vindo a sentir tem gerado novas técnicas e novos produtos com o objetivo de melhorar a qualidade de vida do ser humano. A área da saúde tem sofrido um acréscimo acentuado de equipamentos de tratamento e diagnóstico cada vez menos invasivos e cada vez mais seguros, de forma a proporcionar um aumento da qualidade de vida e a longevidade do ser humano.

Com o objetivo de suprir a vontade inata de viver cada vez mais e melhor, com o menor sofrimento e de forma a proporcionar uma maior qualidade de vida, a área tecnológica aliou-se à inovação e a outros ramos das tecnologias, nomeadamente às áreas de robótica, radiação, bioquímica, biofísica, electromedicina, informática, entre outras.

O termo IoT(internet of thinks) [1] ou Internet das Coisas é uma nomenclatura abrangente, referente aos esforços em curso para interligar uma grande variedade de equipamentos físicos ás redes de comunicação. Atualmente, não se trata apenas de computadores, mas de uma panóplia de equipamentos ligados à rede, nomeadamente TV's, frigoríficos, eletrodomésticos, automóveis, smartphones, camaras de videovigilância, portas, sondas, sensores, entre outros.

O termo Healthcare 4.0 [2] está relacionado com a industria 4.0 que abrange as tecnologias emergentes que ajudam a otimização de tomadas de decisões estratégicas e inteligentes entre elas, seja o IoT, o big data, a computação na cloud, a gestão analítica e a inteligência artificial.

De acordo com a pesquisa realizada em 2018 pela IoT Analytics [3], os dispositivos ligados ao mundo digital já ultrapassam os 17 biliões, sendo que os equipamentos IoT ultrapassa os 7 biliões de equipamentos.

Como se pode observar na figura 1, o número de dispositivos ou equipamentos IoT ligados [4] à rede aumenta gradualmente, sendo esperado que dentro de 6 anos em 2025 este valor ultrapasse os 21 biliões de equipamentos.

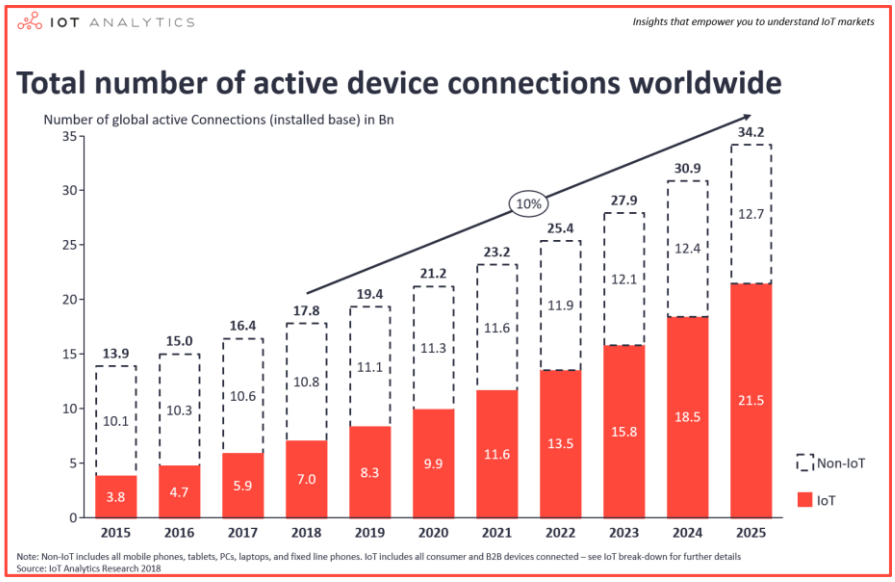

Figura 1 - Número total de equipamentos ligados à internet[5]

Os principais objetivos dos equipamentos IoT focam-se na recolha e na transmissão de dados. O seu tamanho é variado assim como o sistema operativo embutido difere de fabricante para fabricante. Os sistemas operativos embutidos mais utilizados [6] são o "Contiki" (sistema leve de código aberto para sistemas de rede, com mecanismos para o desenvolvimento de softwares para IoT), o "Android" (plataforma de código aberto para equipamentos móveis que inclui, middleware e aplicativos) ou o "TinyOS" (sistema operativo de código aberto para redes de sensores e objetos inteligentes).

Segundo a IoT Analytics [7], as aplicações são diversas, podendo ser utilizadas em casas, em cidades, em redes elétricas, na industria, em fábricas, em veículos, na medicina, na agricultura e onde se justifique modernizar e otimizar os sistemas existentes.

Os benefícios para as unidades de saúde adotarem tecnologias IoT [8] focam-se na redução de custos, uma vez que a monitorização passará a ser feita em tempo real, evitando a deslocalização de um profissional de saúde junto do doente; o resultado do tratamento será melhor, dado existirem indicadores que ajudam na tomada de decisão; consulta de dados em tempo real, possibilidade de abordar uma possível doença no estágio inicial, evitando que esta se descontrole; redução de erros, os fluxos de trabalho são automatizados e combinados com decisões baseadas em vários sensores; melhor experiência para o doente e uma extração de dados com diversos indicadores.

Os equipamentos IoT no ramo da medicina ou da área da saúde têm evoluído bastante, no entanto a segurança destes mesmos equipamentos não tem acompanhado esta grande evolução.

Em 2014 a GE Healhtcare realizou uma investigação, intitulada "O valor do saber" sobre a importância dos avanços tecnológicos para a área da saúde, onde foram entrevistadas mais de dez mil pessoas, em dez países diferentes, concluindo que 90% dos entrevistados afirmam que o uso das tecnologias dará para monitorizar a saúde à distância sendo a mais importante inovação médica dos últimos anos. Passados quatro anos, em 2018, esta tendência confirmou-se.

O grupo Vodafone desenvolveu em 2017 um white paper [9] em conjunto com uma universidade de Liége, na Bélgica onde concluíram que os IoT aplicados à saúde melhoram a qualidade de vida e poupam milhares de milhões de euros aos cofres do estado.

Atualmente, os prestadores de serviços de saúde monitorizam quatro sinais vitais: a temperatura do corpo, a pulsação, a respiração e a tensão arterial. É notório que os IoT estão em evolução constante, sendo que em breve poderão medir de forma rigorosa mais indicadores.

A combinação de sensores, equipamentos móveis e machine learning dos equipamentos, fornece uma infinidade de informações sobre sintomas de doentes em tempo real para clínicos e pesquisadores tendo dado origem ao Projeto Blue Sky [10], de uma parceria entre a Pfizer e a IBM. Este projeto tem como principal função ajudar os doentes de Parkinson a lidar com a doença, proporcionando uma melhor e maior qualidade de vida.

A higiene em ambientes hospitalares é também uma questão que necessita de ser encarada com muito rigor, assim de forma a minimizar o risco de infeção e possíveis contaminações foi desenvolvido um sensor que verifica as pessoas que se encontram numa sala, e monitoriza quantas desinfetaram as mãos. Estes sensores recolhem esta informação e criam indicadores de qualidade. Esta tecnologia foi desenvolvida pela Gojo [11] em pareceria com a Microsoft.

Ainda neste âmbito da infeção hospitalar, a empresa Intelligentm [12] criou uma pulseira com RFID que verifica a proximidade do dispensador de desinfetante e graças ao giroscópio verifica a forma como os profissionais de saúde lavam as mãos. De seguida os dados são analisados, tratados e é determinada a eficiência da lavagem de mãos com o índice de infeção hospitalar, conseguindo assim reduzir este valor.

A empresa Novartis em pareceria com a gigante Google [13] criaram uma lente de contacto que avalia os níveis de glicose dos doentes diabéticos recolhendo e tratando esta informação. Estes dados ajudam o doente a regular os seus índices de açúcar no sangue e disponibilizam automaticamente a dose de insulina que deverá ser administrada.

Os equipamentos de diagnóstico desempenham um papel vital para ajudar na melhoria de prestação de cuidados de saúde, nesse âmbito a Roche [14] explorou o uso da tecnologia dos IoT para monitorizar os equipamentos de diagnóstico (IVD), otimizando a disponibilidade dos equipamentos que tem nos diversos laboratórios hospitalares.

Em 2016, o organismo que controla os alimentos e os medicamentos nos EUA [15] aprovou o MiniMed 670G. Este dispositivo também permite monitorizar automaticamente a glicose automaticamente no doente e fornece ao equipamento as doses de insulina necessárias. Esta tecnologia está dotada de um sensor que analisa a glicose e imediatamente transmite esta informação para a bomba por uma tecnologia sem fios.

De forma a preservar o transporte de vacinas e a garantir o seu acondicionamento correto, a Weka [16] criou uma arca térmica com sondas de temperatura que mantem a temperatura estável em função da temperatura exterior. Estas sondas conseguem criar um ambiente estável, existindo apenas uma gaveta que fornece a vacina, protegendo as vacinas da temperatura exterior. Este equipamento envia a informação do lote fornecido assim como faz uma gestão de stock permitindo uma rastreabilidade da vacinação.

Utilizando também sensores de temperatura, a BTT Corp [17] desenhou uma fita que analisa e captura a temperatura do cérebro de forma não invasiva e continua, possibilitando um estudo aprofundado para perceber como o organismo reage à medicação.

A Zion China [18] empresa de serviços móveis da saúde e telemedicina, em Pequim, desenvolveu uma ferramenta de monitorização de glicose no sangue. Esta ferramenta recolheu 3000 leituras durante sete dias. Nesse mesmo período de tempo esse sensor recolheu também dados sobre os hábitos de alimentação, exercício físico e medicação dos pacientes.

O hospital alemão Ruppiner Kliniken [19], criou um equipamento que recolhe informação diária do paciente relativamente a eletrocardiogramas (ECG) e a tensão arterial. Esta informação é armazenada e depois é analisada por cardiologistas de forma a perceber qual o

estado cardíaco do doente, emitindo alertas (sonoro, mensagem de texto ou até mesmo telefónico) se existirem valores que necessitem de presença médica imediata junto do doente.

Uma pesquisa do Ponenon Institute's [20] revelou que 39% dos fabricantes dos equipamentos médicos assumiram que uma pessoa mal intencionada conseguiu assumir o controlo de um equipamento e que apenas 15% das organizações de atendimento médico confirmam que estão a tomar medidas significativas para evitar ataques.

Em março de 2019 [21], o departamento de segurança interna dos EUA publicou um alerta para pacientes com desfibriladores cardíacos, alegando que os ciberatacantes conseguiriam sequestrar remotamente e colocando em risco a vida de milhões de pessoas. Como principais falhas está a falta de autenticação e a ausência de criptografia.

Existem variadíssimos IoT já em uso na área da saúde, tornando os hospitais ou as unidades de saúde mais eficientes, nomeadamente na monitorização do atendimento e tratamento de utentes no domicílio, na monitorização cardíaca com alarmística, utilizando variadíssimos sensores ou programas terapêuticos que monitorizam a atividade cerebral no paciente.

Em âmbito hospitalar os sistemas e aplicações ligados á internet ou á rede são variadíssimos, como por exemplo as bombas de insulina, os pacemaker, os dispensadores de medicamentos, as estações de aquisição de imagem, as UPS (uninterruptible power supply), as impressoras, os controladores de autómatos (responsável, por exemplo, para o quadro geral baixa tensão - QGBT), as camaras de videovigilância, os controlos de acesso (biométrico, os cartões de proximidade RFID), as pulseiras anti rapto, os quiosques de pagamento automático, a central telefónica, o aparelhos de picking, entre outros.

Dos exemplos apresentados verifica-se que os IoT fazem parte do nosso quotidiano, ajudando os profissionais que exercem as suas funções numa unidade de saúde a recolher um conjunto de informação, minimizando o risco nos seus processos diários e otimizando os mais variados processos.

Com a crescente transformação digital o IoT tem possibilitado uma melhoria dos procedimentos de diagnóstico e de monitorização, reduzindo os gastos nos cuidados da saúde.

Em fevereiro de 2018 foi formalizado um memorando de entendimento entre a empresa tecnológica Cisco e um hospital do norte [22], que visa a criar o primeiro "Smart Hospital"

da europa. Este hospital inteligente irá melhorar a experiência e o conhecimento dos IoT no mercado da saúde.

Recentemente, em junho de 2019 a Medtronic [23] o governo dos Estados Unidos e o Infarmed [24] emitiram um alerta que algumas bombas de insulina MiniMed da Medtronic eram vulneráveis a ataques, sendo possível explorar uma falha de software e injetar, reproduzir ou modificar os dados da bomba, podendo ser possível tomar controlo sobre a dosagem a administrar tendo esta falha ficado registada com o CVE-2019-10964.

De acordo com a consultora Gartner [4], em 2020 existirá mais de 20 biliões de equipamentos ligados á internet, pelo que será necessário novas ferramentas para analisar os tráfegos e gerir equipamentos obsoletos.

Um dos desafios dos IoT passa pela correta inventariação dos equipamentos ligados à rede. Assim, e de forma a saber o que existe ligado é de todo fundamental o auxílio de aplicações que permitam a inventariação dos demais equipamentos presentes na rede.

Existem também alguns programas ou aplicações que efetuam testes de vulnerabilidades á rede e verificam se os sistemas estão seguros, nomeadamente: OpenVas, Nessus, Nexpose, Secapps, W3af, Wapiti, WebReaver, DVCS Ripper, Arachni.

Apesar destas aplicações efetuarem uma identificação fiável, existem muitos equipamentos que não são catalogados da maneira mais assertiva nem contemplados para análise e por consequência podem não ser detetadas vulnerabilidades conhecidas existindo muito falso positivo antes da sua catalogação.

Assim, cabe ás equipas locais de tecnologias de informação, uma inventariação correta e uma monitorização constante dos equipamentos presentes na rede que gerem, sendo fulcral que procedam a atualizações de segurança sempre que tal se justifique.

A Associação Americana de Hospitais [25] identificou que os equipamentos médicos com ligação à internet melhoram significativamente o atendimento e a eficiência do utente, no entanto também verificaram que estes equipamentos são mais suscetíveis a ataques. Este crescente número de ataques motiva a necessidade de identificar os riscos e as vulnerabilidades dos equipamentos de forma a evitar incidentes que ponham em risco a vida humana.

2.1. Tipos de Comunicação

Os protocolos de rede e os tipos de comunicação tem evoluído e aparecido no mercado à medida que os equipamentos IoT surgem e amadurecem. As taxas de transferência, ou número de nós que permite ligar em simultâneo, assim como da distância do gateway, estão na origem de novos e variados tipos de comunicação.

Os diversos dispositivos que formam os equipamentos IoT são limitados ao nível de recursos, no entanto a sua forma de comunicação é muito heterogénea e a forma como comunicam difere de equipamento para equipamento.

Os métodos para recolha de informação tem evoluído conforme as formas de comunicação ganham maturidade, aumentando assim a utilização e a proliferação de equipamentos ligados à internet.

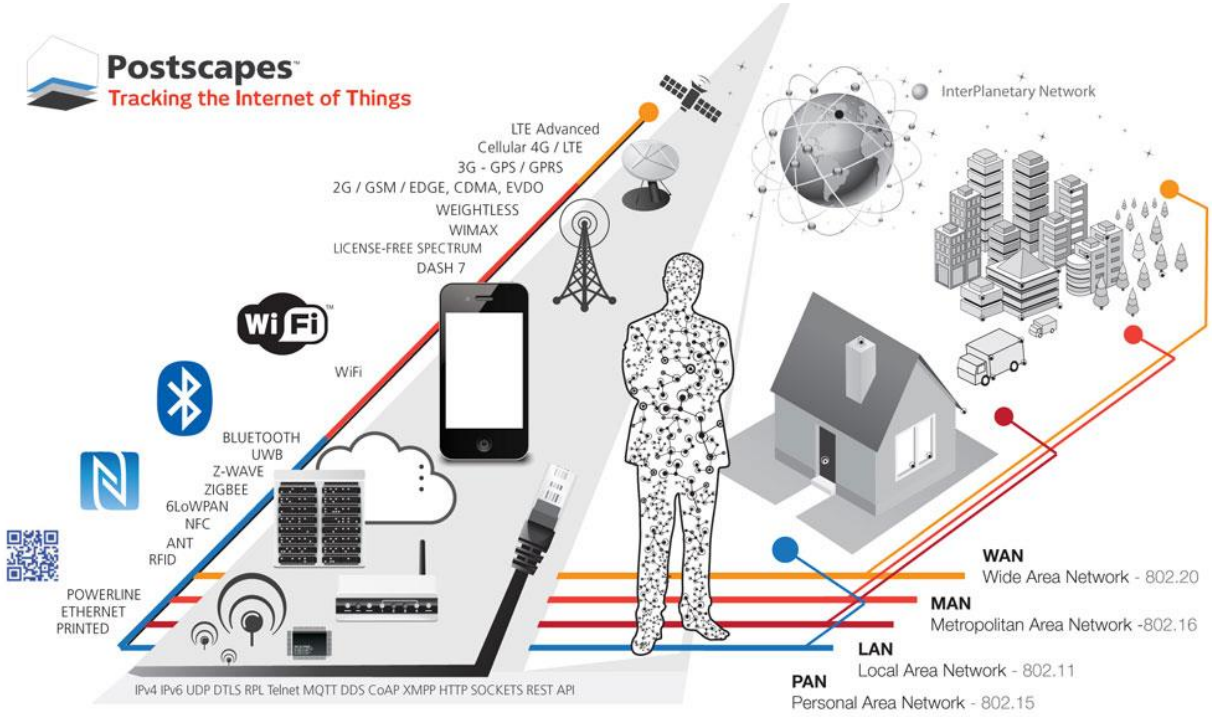

Figura 2 - Diagrama de conectividade[26]

A figura 2 apresenta as diversas formas de transmitir a informação recolhida, tais como o wi-fi, o Bluetooth, o NFC, entre outros, bem como o espectro de alcance dessa informação, passando das redes pessoais (PAN), onde se considera a utilização de um monitor cardíaco, ou um dispositivo móvel, redes locais (LAN), redes metropolitas (MAN) ou redes de longa distância (WAN). Esta figura demonstra também como o IoT se vem enraizando na nossa

sociedade, evidenciando a ideia cada vez mais adotada de que a informação pode ser proveniente de qualquer "coisa".

Como se pode constatar é notável a crescente evolução das mais variadas tecnologias pelo que se tem verificado que estas têm acompanhado as necessidades dos variados negócios onde se enquadram. Os fabricantes têm tentado responder ás solicitações que lhes são pedidas, pelo que diariamente aparecem novos produtos com novas funcionalidades e vários propósitos.

Na figura 3 está presente a evolução dos demais protocolos ao longo dos anos. Durante este período o âmbito de ação também foi alargado, assim como existiu um crescimento e o aparecimento de novos sistemas e funcionalidades.

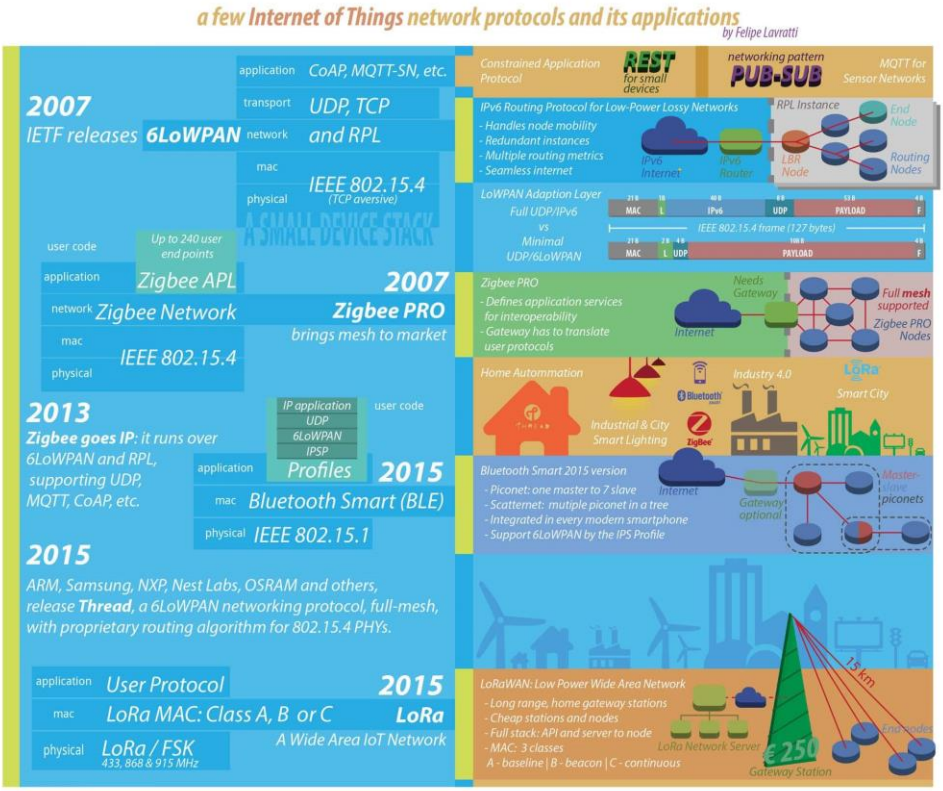

Figura 3 - Protocolos de rede IoT e sua aplicação[27]

Hoje em dia existe a necessidade de se estar ligado ao mundo, de ver mais alem e as demais tecnologias têm acompanhado essas espectativas e dado resposta aos utilizadores.

Com o rápido desenvolvimento das Internet das Coisas, a monitorização da saúde tem adquirido novos *players* no mercado, contudo a introdução destes novos equipamentos tem

trazido novos desafios, sendo que uma das principais preocupações foca-se nos protocolos de comunicação [28].

Elencam-se assim os principais protocolos de comunicação de equipamentos IoT:

2.1.1. 6LowPAN

O 6LowPan [29] [30] é um protocolo IP (Internet Protocol). O nome é a abreviatura de IPv6 Low-power wireless Personal Area Network. A pesar de ser uma tecnologia IoT como Bluetooth ou ZigBee, o 6LowPAN é um protocolo de rede que define o encapsulamento, headers e com mecanismos de compressão. O atributo chave é o IPv6 stack, que foi um passo muito importante para viabilizar a Internet das Coisas. Com o IPv6, é possível atribuir a cada objeto ou equipamento do mundo o seu IP único e liga-lo assim à rede ou à internet.

Este tipo de comunicação [31] veio remover alguns cabeçalhos IPv6 e UDP por estes possuírem valores conhecidos, nos casos mais comuns na utilização das redes de sensores, apenas um número limitado de portas é utilizado, de modo que quatro bits são suficientes para descrevê-las, em vez dos normais 8 bits.

2.1.2. ZigBee

O Zigbee [32] é um dos protocolos mais usados, com aplicações mais focadas para ambientes industriais do que residenciais. É baseado no padrão IEEE802.15.4, que é um padrão para redes wireless na faixa de 2.4GHz. As aplicações, geralmente não requerem mudanças constantes na taxa de transmissão. Todos os principais fabricantes de semicondutores possuem módulos Zigbee nos portfólios que comercializam. O alcance deste protocolo vai dos 10 aos 100 metros e a taxa de transmissão alcança um máximo de 250kbps. O protocolo é atualmente mantido pela empresa Zigbee Alliance.

2.1.3. Bluethooth

O protocolo é mantido pela empresa Bluetooth SIG (Special Interest Group) [33], e possui uma extensa documentação e exemplos de aplicações disponíveis na internet, o que facilita muito a integração da tecnologia em projetos de automação residencial, comercial e produtos eletrónicos no geral. O alcance deste protocolo varia conforme a classe do módulo. Os chips da classe 1 têm alcance de até 100 metros e potência de 100 mW. Os módulos da classe 2 têm alcance de até 10 metros e potência de 2,5mW. Já a classe 3 tem alcance de apenas 1

metro e dissipa no máximo 1 mW. O Bluetooth 5.0 tem alcance de até 240 metros e taxa de transmissão de 50 Mbit/s.

Quando os equipamentos estão no raio de alcance, eles podem ser encontrados independentemente da sua localização, permitindo que funcionem em ambientes diferentes, dependendo da potência do dispositivo.

2.1.4. Wi-Fi

As redes wi-fi funcionam com o padrão IEEE 802.11.b,g,n [34] , 2.4 GHz e 5 GHz e utilizam sinal de Radio Frequência para difusão, são consideradas redes de alta qualidade e de alta flexibilidade indicadas para utilização a médias distâncias (dezenas de metros). É uma tecnologia que possui uma evolução de altas taxas (Gbps) de comunicação.

Este tipo de comunicação permite a transmissão de dados para computadores, portáteis, telemóveis, tablets, entre outros equipamentos com este tipo de tecnologia de forma simultânea e permite uma liberdade de utilização, não estando limitado a uma zona, uma vez que o seu alcance é amplo.

2.1.5. RFID

O RFID - Radio-Frequency IDentification [35] utiliza campos magnéticos para automaticamente identificar e rastrear as etiquetas ou em inglês as t*ags* que são coladas nos objetos. Os sistemas RFID incluem equipamentos eletrónicos denominados de transponder ou tags e leitores que comunicam com essas etiquetas. As tags RFID contêm antenas para permitir receber e responder a pedidos por radiofrequência, não necessitando de alimentação elétrica para funcionarem. A frequência varia dos 100 KHz aos 5,8 GHz e o alcance varia dependendo do leitor podendo chegar aos 8 metros.

2.1.6. NFC

Near Field Communication (NFC) [36], é uma tecnologia utilizada para troca de informações entre dois equipamentos eletrónicos. É uma extensão da tecnologia de cartões RF (RFIDs) que permite aos equipamentos trocar informações, desde que dentro de uma distância máxima, que costuma ser de poucos centímetros. As taxas de transmissão vão de 100 até 420 kpbs. O padrão NFC está estabelecido pela norma ISO/IEC18000-3. É uma tecnologia

que permite a troca de informações entre equipamentos sem existir a necessidade de cabos, no entanto é necessária uma aproximação física para uma correta leitura e o reconhecimento da informação, uma vez que o alcance geral do protocolo é de 10 cm.

2.1.7. Thread

Foi lançado em 2014 pelo Thread Group [37] e é baseado em vários padrões, incluindo o IEEE802.15.4, IPv6 e 6LoWPAN. Oferece uma solução do tipo IP para IoT em âmbito residencial. Este tipo de comunicação possibilita gerir uma rede com até 250 nós.

2.1.8. LoRaWAN

O protocolo LoRa[38] foi desenhado para comunicações de baixo consumo energético. Mantido pela LoRa Alliance, esse protocolo suporta redes amplas com milhões de equipamentos e possui velocidade entre 0.3 kbps até 50 kpbs. É um dos protocolos IoT mais populares.

A seguinte tabela apresenta uma comparação dos diversos tipos de comunicação utilizados pelos equipamentos IoT, relativamente á frequência, ao alcance, à autonomia, tipologia e nós:

Tecnologia	Standard	Rate/ Frequency	POWER	Alcance	Bateria	Tipologia	Nós
WI-FI	IEEE 802.11b	54 Mbps	400/ 20 mA	1-100m	Horas	Estrela	64+190
RFID	ISO/IEC 18000	125Khz, 13,56Mhz 800Mhz a 960Mhz 2,45Ghz ou 5,8Ghz	-	Metros	-	Estrela	7
ZIGBEE	IEEE 802.15.4	20 to 250 Kbps	30mA/ 356uA	100+m	Meses/ Anos	STAR	32
BLUETOOTH	IEEE 802.15.1	1 Mbps	49mA/ 0,2mA	1-10 m	Dias	P2P/STAR	254 A 64516
NFC	ISO/IEC 18092	424 Kbps	-	1-10 cm	Meses/ Anos	1 + 1	2
6LowPAN	IEEE 802.15.4	868-868.6 MHz 902-928 MHz 2400-2483.5 MHz		10 a 100m	Anos	Estrela / Malha	
Thread	IEEE 802.15.4	2.4GHz	400 mA	10 cm		Estrela	250
LoRaWAN	IEEE 802.11ah	109 MHz, 433 MHz, 866 MHz e 915 MHz		2km a 45km		Estrela	

Tabela 1 - Comparação dos Tipos de Comunicação [39]

2.2.Protocolos de comunicação

Na medida em que as tecnologias vão evoluindo, também vão surgindo novos protocolos para se adequarem ás necessidades destas tecnologias, tornando as comunicações mais fluidas e transmitindo o essencial em função do propósito a que se destinam.

Elencam-se assim os principais protocolos utilizados nas comunicações dos equipamentos IoT:

2.2.1. MQTT - Message Queue Telemetry Transport

O MQTT[40] foi criado pela IBM nos anos 90 para ser utilizado em sistemas de supervisão e aquisição de dados num panorama industrial, o SCADA (Supervisory Control and Data Acquisition.

É um protocolo baseado no modelo publicação-subscrição de mensagens [41] e projetado para funcionar em TCP. O protocolo consome poucos recursos e foi desenhado para suportar redes com falhas e de forma intermitente.

2.2.2. CoAP – Constrained Application Protocol

Em junho de 2014 foi publicado o RFC 7252[42] que propõem o CoAP[43] como um protocolo de troca de mensagem direcionado para equipamentos com restrições de processamento, memória e energia, para redes de baixa largura de banda que utiliza o modelo ‘cliente/servidor’, e disponibiliza uma interação unilateral ‘request/response’.

Este protocolo difere do protocolo MQTT, uma vez que o CoAP surgiu para operar diretamente com o protocolo HTTP. Segundo [42] este protocolo possibilita a troca de mensagens assíncronas, tem capacidades simpres de proxy e de cache e suporta métodos de GET, POST, PUT e DELETE. Estes métodos permitem facilmente obter, colocar, enviar ou apagar dados facilmente entre dois equipamentos.

2.2.3. HTTP - HyperText Transfer Protocol

O HTTP[44] foi especialmente desenhado para a internet em 1997. O HTTP é um protocolo simples baseado em texto sem tamanho fixo para o cabeçalho. Possui características para ligações persistentes e não persistentes. Por defeito, é utilizado TCP como protocolo de transporte do HTTP.

Trata-se de um protocolo muito poderoso[45], no entanto utiliza demasiados recursos de rede o que dificulta a sua adoção em equipamentos IoT.

2.3.Normas de comunicação

A definição de normas standard ou a padronização das comunicações já há largos anos que tem vindo a ser implementada, no entanto não tem sido aplicada na sua totalidade uma vez que cada fornecedor cria o seu próprio mercado. Com a interoperabilidade a ganhar terreno, este tipo de padrão tem ganho cada vez mais adeptos e as aplicações clínicas e os equipamentos médicos começaram a comunicar com os standard mais comuns nesta área, são eles o HL7, o DICOM e o OpenEHR.

2.3.1. HL7 – Health Level Seven

O Protocolo HL7[8] é um protocolo de transmissão de mensagens entre equipamentos médicos, sistemas de informação e bases de dados clínicas, que define um conjunto de regras e formatos e que garante a interpretação da informação independentemente da fonte.

O HL7[46] é uma framework standard, desenvolvido por uma organização sem fins lucrativos, denominada Health Level Seven, fundada em 1987 e certificada pelo ANSI (American National Standards Institute) para desenvolver padrões para a área da saúde desde 1994 (Health Level Seven, 2017).

Em Portugal o protocolo HL7 é usado e reconhecido[47] como norma aceite pelo estado, empresas de software e pelas empresas que produzem equipamentos médicos para facilitar a partilha de dados entre soluções heterogéneas.

2.3.2. DICOM - Digital Imaging and Communications in Medicine

As normas DICOM [48] vieram permitir que a transmissão de imagem fosse efetuado com um padrão em todo o tipo de exames uma vez que as imagens são armazenados num único formato possibilitando que estas possam ser visualizadas por equipamentos de marcas distintas.

Esta normalização veio permitir uma maior nitidez nas visualizações das imagens, possibilitando um melhor diagnóstico.

Esta norma também possibilita confirmar se uma determinada imagem foi gravada ou transmitida com sucesso, garantido que nenhum arquivo é perdido.

2.3.3. OpenEHR

O openEHR [49] é um conjunto de especificações de código fonte aberto para registos eletrónicos de saúde. O resultado é uma referência internacional para a criação de modelos de conteúdo clínicos (baseado no padrão ISO 13606), proporcionando a interoperabilidade da informação clínica entre diferentes sistemas de saúde

Esta norma propõe uma metodologia de desenvolvimento em dois níveis, sendo uma ao nível de software e outra ao nível da camada de conhecimento clínico.

2.4. Ataques de Segurança

Os ataques de segurança a unidades de saúde ocorrem com frequência. Um dos exemplos mais recentes remonta a fevereiro de 2019, onde um ataque de ransomware aconteceu no Melbourne Heart Group[50]. Esta unidade viu toda a sua informação constante nos servidores a ser encriptada por cibercriminosos. Outro ataque bastante relevante aconteceu o ano passado com o sistema de saúde de Singapura. O SingHealth[51] foi vítima de uma fuga de informação massiva onde constavam os registos de saúde do Primeiro Ministro, seguido do roubo dos registos de 16 mil pacientes do UnityPoint[52] umas semanas depois. Também em maio de 2017 assistiu-se ao ataque WannaCry[53] que resultou no cancelamento de mais de 19 mil consultas no Serviço Nacional de Saúde do Reino Unido e no gasto de mais de 150 milhões de libras na tentativa de solucionar a situação.

Devido à grande quantidade de informação pessoal que foi possível roubar e transferir eletronicamente, as organizações de saúde tornaram-se nos principais alvos dos cibercriminosos que, para além de quererem causar disrupção em massa, também pretendem lucrar com o ataque que originam.

Um sistema IoT pode ser atacado das mais variadas maneiras, de tal forma que o ataque pode ser físico, dentro da própria rede ou com recursos a outros equipamentos. Como os equipamentos IoT são implementados em tecnologias de redes diferentes, existe uma necessidade de efetuar uma catalogação adequada dos ataques para se desenvolverem medidas preventivas ou de mitigação de ataque.

A tabela 2 resume a classificação [54] dos ataques de equipamentos IoT:

Ataques físicos	**Ataques de rede**	**Ataques de software**	**Ataques de criptografias**
Alteração de Nós	Análise de Tráfego	Vírus	Ataque de texto cifrado
Injeção de nó malicioso	Eavesdropping	Spyware	Ataque de código cifrado
Injeção de código malicioso	Message Injection	Adware	Man-in-the-midle
Engenharia Social	Message Replication	Cavalo de Troia	Ransomware
Radio Jamming	Sinkhole Attack	Scripts Maliciosos	
Node Destruction	Sybil Attack	DoS	
Hello Flooding	Message Alteration	Malware	
Black Hole Attack	DoS		
Wormhole Attack	RFID Spoofing		
Slowdown	RFID Cloning		
	Man-in-the-midle		

Tabela 2 - Classificação de Ataques em IoT [55]

2.5. Tipos de Ameaça

Qualquer dispositivo ligado à rede está suscetível de ser atacado, quer por fins comerciais, quer por fins destrutivos, vandalismo ou terrorismo, ou então simplesmente para se pesquisar vulnerabilidades dos sistemas, dos servidores ou dos equipamentos interligados. Este tipo de pesquisa de vulnerabilidade tem como principal objetivo melhorar a segurança do mesmo.

Apesar do potencial do IoT em todos os eixos em que opera, a infraestrutura de comunicação dos equipamentos IoT tem falhas conhecidas do ponto de vista da segurança [56] [57], pelo que é suscetível a quebras na privacidade dos dados transmitidos.

De acordo com os estudos efetuados [58] pela ENISA Threat Taxonomy42 [59] elencou-se uma lista com as principais ameaças:

2.5.1. DoS

O DoS [60] é a designação de Denial Of Service. É um ataque de negação de serviço e que pode ter como alvo um sistema IoT, resultando assim na indisponibilidade e na interrupção da produção causada por um elevado número de pedidos enviados para o sistema.

Segundo o RFC 8576 [61] os equipamentos IoT implementam mecanismos para verificar as rotas de retorno com base na análise de cookies para atrasar a resposta do host, no entanto estes mecanismos de defesa podem ser infrutíferos dado que quem ataca tem mais capacidade de processamento do que o equipamento que está a ser atacado.

2.5.2. Malware

Trata-se da penetração de software malicioso, destinado a realizar ações não autorizadas, podendo causar danos no equipamento ou na rede. O ransomware[1], vírus, cavalos de troia e spyware[2] são exemplos comuns desta ameaça.

2.5.3. Manipulação de hardware ou software

Este tipo de ameaça foca-se na manipulação não autorizada do equipamento, alterando e modificando as suas configurações e a génese ou o propósito para que se destina.

São ataques que alteram o código fonte do equipamento criando a ilusão de que o equipamento está com o comportamento normal, mas poderá estar a efetuar outras tarefas, como por exemplo o envio de uma cópia dos dados para outro local ou servidor.

2.5.4. Manipulação da informação

A manipulação da informação pode acontecer, se um atacante se colocar a capturar o tráfego de rede e o entregar alterado ao seu destinatário. Este tipo de ataque por norma denomina-se Man-In-The-Midle, podendo também este tipo de manipulação ser efetuado por uso de malware destinado a esse fim. É um ataque transparente para o utilizador final de difícil deteção.

2.5.5. Brute Force

A ameaça de obter acesso não autorizado a um ou vários recursos da organização, através de um ataque de força bruta. Este tipo de ataque vai tentado adivinhar as credenciais corretas para aceder a dispostitos ou servidores não autorizados tornando os sistemas vulneráveis.

[1] Tipo de software nocivo que restringe o acesso ao sistema infetado encriptando os dados de um sistema e que solicita um resgate em cripto moedas para resgate da informação.
[2] Aplicação que se permanece instalada no sistema operativo para espiar o utilizador, fornecendo informações ao seu autor.

Este tipo de ataque é um ataque demorado, que numa primeira instância efetua testes com as credenciais padrão dos equipamentos, passando por ataques com o recurso ás palavras de dicionário, e numa fase mais avançada, poderá ser efetuado um ataque de engenharia social de forma a perceber quem opera com determinados acessos focando o ataque para esse utilizador.

2.5.6. Ataques direcionados

Os ataques direcionados, tem como objetivo roubar informação em alvos específicos. São ataques que são planeados e estruturados podendo demorar dias, meses ou semanas a planear e a implementar para surtir o efeito desejado.

2.5.7. Reconhecimento de rede

O reconhecimento de rede [62] tem como principal função validar a ligação dos nós na rede, enumerar os serviços que se encontram ativos e verificar por vulnerabilidades nas aplicações. Este tipo de snife faz um pesquisa a todos os nós ligados na rede, identificado com detalhe, algumas características do equipamento, nomeadamente as portas e o ip onde conseguiu acesso.

2.5.8. Man-in-the-Middle

Um ataque Man-in-the-middle é um nome genérico que se dá a um ataque virtual em que o intruso ou o atacante fica no meio da comunicação, pelo que é capaz de receber, ler, e enviar a informação para o destino. Este tipo de ataque permite que os dados saiam do recetor, sejam analisados pelo intruso e de seguida enviados para o destinatário, sem que ambos se apercebam que houve espionagem de informação, sendo também possível a manipulação da informação antes do reenvio para o destinatário.

2.5.9. Vandalismo ou terrorismo

Os dados existentes numa rede informática podem ser alvo de vandalismo, de forma a impactuar indisponibilidade ou pedido de resgate monetário. Esta forma de terrorismo pode inviabilizar o modelo de negócio de uma instituição causando prejuízos elevadíssimos, quer monetário, como vitais.

2.5.10. Sabotagem

A sabotagem impede o pleno funcionamento de qualquer sistema, causando indisponibilidade. As formas de prejudicar o normal funcionamento podem ser variadíssimas, nomeadamente com a falha de luz, o corte físico de cabos, o curto-circuito induzido, entre outros.

2.5.11. Ataques de Botnets

Os ataques de botnets ocorrem utilizando por norma Cavalos de Troia para violar a segurança do sistema. Estes robots executam tarefas de maneira autónoma e automática proporcionando a negação de serviço ou o acesso a informação privilegiada. São na sua maioria, ficheiros normais de vídeo, áudio, foto, texto ou folhas de cálculo que trazem embutidos estes agentes que despoletam outras ações não solicitadas pelo utilizador.

2.5.12. Exploits de vulnerabilidades

Neste tipo de ameaça o invasor aproveita falhas de firmware ou de software do dispositivo. Os equipamentos IoT são frequentemente vulneráveis devido à falta de atualizações, uso de passwords por defeito ou configuração imprópria. Atualmente existem bibliotecas atualizadas das vulnerabilidades mais comuns para cada equipamento, onde é facilmente identificado se determinado equipamento cumpre com determinada falha ou requisito, podendo ser explorado as vulnerabilidades elencadas.

2.5.13. Negligência dos funcionários

A negligência dos funcionários é também uma das ameaças comuns nas organizações, uma vez que a cultura de segurança está pouco incutida e existe muito facilitismo entre os colegas de trabalho. Assim é frequente a partilha de passwords para acesso ao computador, os funcionários não estão formatados a bloquear o posto de trabalho quando se ausentam nem a alterar as passwords fornecidas aquando do primeiro acesso e por norma a salvaguarda de passwords é feita em post-its. Estes exemplos de negligência interna podem inadvertidamente comprometer a segurança das organizações.

Na secção que se segue serão abordados alguns tipos de equipamentos IoT que podem ser encontrados em organizações ou em unidades de saúde, alertando para os riscos e as

vulnerabilidades que cada um acarretam em caso de utilização despreocupada ou sem regras, sendo evidenciado alguns ataques a que estão propensos.

2.6. Riscos dos Equipamentos IoT

O IoT possui um vasto leque de possibilidades de utilização, sendo que é necessário ter consciência dos problemas que estes poderão proporcionar no futuro. Este capítulo aborda os riscos dos equipamentos IoT e a necessidade de se efetuar essa correta identificação.

A identificação dos riscos é uma tarefa muito importante para que se possa entender como e onde agir, mitigando ou eliminando qualquer especto de segurança ou privacidade de dados que possa advir da incorreta utilização destes equipamentos.

Os IoT ligados à rede na área de saúde [63] são potenciais alvos atraentes para hackers, cibercriminosos ou pessoas mal intencionadas pelas mais variadas razões:

- As organizações de saúde têm muitos equipamentos ligados à rede e pode haver lacunas de segurança num determinado equipamento;
- Os equipamentos IoT pessoais transportados pelos utentes, famílias e ou funcionários não são analisados pelas equipas de sistemas de informação locais;
- Estes equipamentos contêm informações valiosas tais como dados pessoais e histórico de saúde pessoal, que podem ser exploradas para obter um determinado lucro.

Este novo paradigma do IoT caracteriza-se por adicionar novos objetos/coisas ligadas às redes, inclusive com ligação à internet, na maioria das vezes com baixo custo, no entanto qualquer objeto inteligente ligado ás redes poderá ou não ser controlado através de um computador remoto ou um smartphone.

As aplicações IoT estão em crescente expansão sendo que diariamente surge um novo aplicativo, um novo sensor ou uma nova funcionalidade. A cada novo desenvolvimento surgem novos desafios ao nível de segurança que necessitam de ser ultrapassados de forma a garantir a confiabilidade, integridade e disponibilidade dos dados transmitidos e recolhidos.

Numa pesquisa publicada pelo HIPAA Journal [64], 89% dos executivos de saúde disseram que sofreram uma violação de segurança resultante da adoção da IoT, enquanto 49% disse que o malware é um problema [65].

As unidades de saúde enfrentam um desafio único quando se trata de segurança da informação. Estas instituições são um emaranhado de "sistemas de sistemas" com enormes matrizes de equipamentos interligados entre si.

Esta situação cria múltiplos pontos de entrada para a rede, tornando a gestão difícil e criando uma ampla superfície de ataque para os cibercriminosos.

Segundo o NIST [66] [67], as ameaças da cibersegurança podem ter um impacto negativo nas redes das organizações e unidades de saúde, assim como nos equipamentos IoT ligados na rede. No entanto estes equipamentos podem ser afetados comprometendo o desempenho do work-flow hospitalar, impedindo procedimentos clínicos ou a indisponibilidade de prestar cuidados de saúde.

O potencial de riscos que os novos equipamentos IoT oferecem é tão grande que a comunidade “OWASP Internet of Things” [68] elaborou o projeto para ajudar os fabricantes, desenvolvedores e consumidores a entender melhor as questões de segurança associadas aos equipamentos IoT, e a consciencializar que os utilizadores devem tomar melhores decisões de segurança aquando da criação, adoção ou implementação de IoT.

Em dezembro de 2018 o OWASP divulgou a lista dos 10 principais riscos de IoT para 2019, apresentando a seguinte imagem:

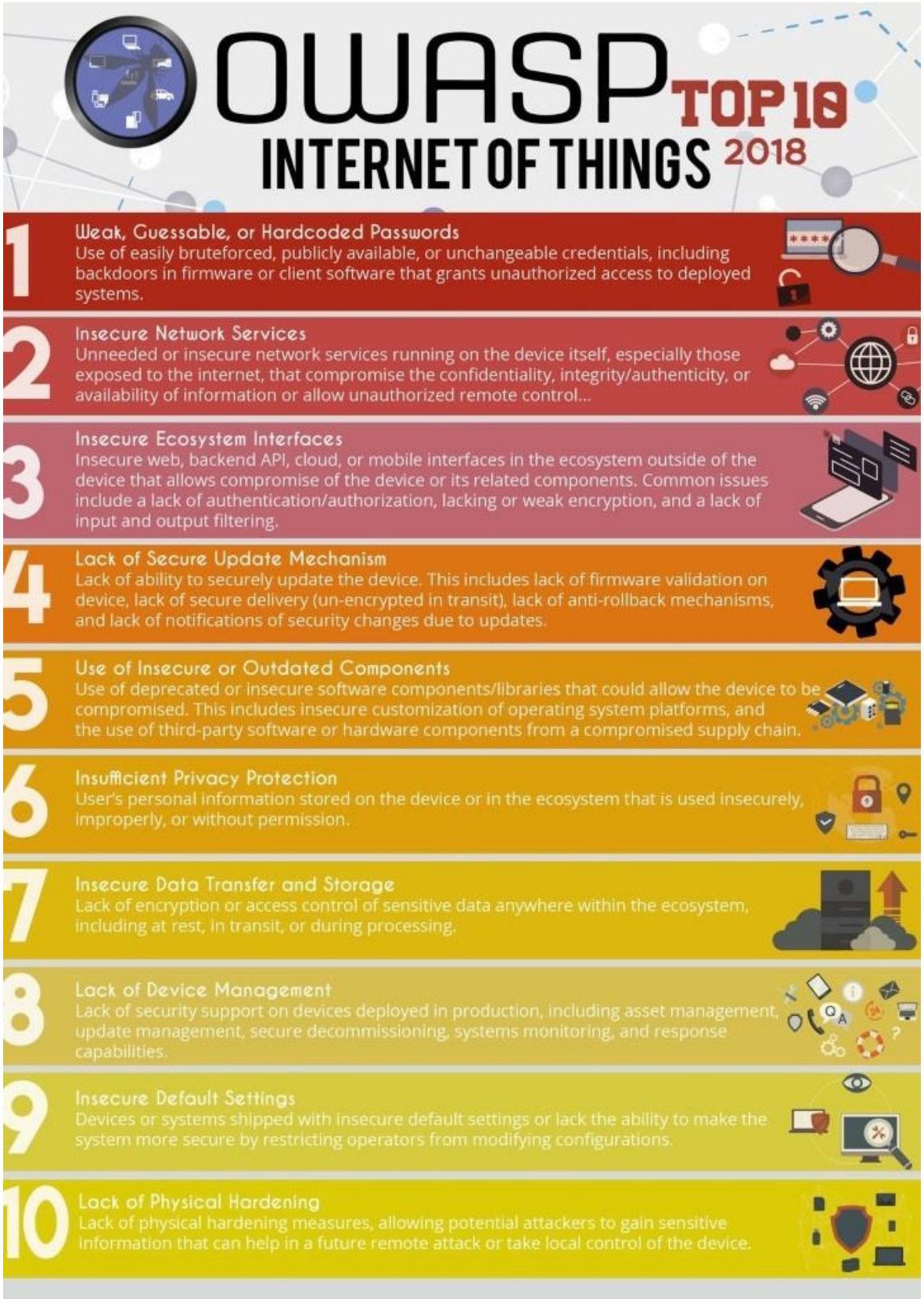

Figura 4 - OWASP Top 10 vulnerabilidades[69]

Tal como verificado na figura 4, o potencial de riscos é elevado por inúmeros fatores, mas existem pontos de vital importância que carecem de avaliação e de uma melhor compreensão. A lista do Top 10 da OWASP para a IoT assenta nos seguintes vetores:

1 - Senhas fracas, fáceis de adivinhar ou codificadas:

A utilização de passwords pode ser facilmente submetida a um ataque bruteforce, uma vez que existem listagens que estão publicamente disponíveis e que são transversais á maioria dos equipamentos.

2 - Serviços de rede inseguros:

Serviços de rede desnecessários ou inseguros executados no próprio dispositivo, especialmente os que estão expostos à internet, que comprometem a confidencialidade, a integridade, a autenticidade ou a disponibilidade de informações ou permitem o controlo remoto não autorizado do dispositivo.

3 - Interfaces inseguras:

Os problemas comuns que incluem falta de autenticação ou de autorização, a criptografia fraca e a falta de filtragem de conteúdos na entrada e saída, capacitam as plataformas web inseguras, assim como as APIs de backend, na nuvem ou os interfaces móveis no ecossistema fora do dispositivo, permitindo o acesso a um dispositivo ou aos seus componentes.

4 – Ausência de mecanismos de atualização:

A capacidade de atualizar o dispositivo com segurança não inclui a validação de firmware no dispositivo, e não valida se a disponibilização deste firmware é entregue em segurança (ausência de criptografia), existe também falta de mecanismos anti-rollback e falta de notificações nas alterações de segurança devido a atualizações.

5 - Utilização de componentes inseguros ou desatualizados:

A utilização de componentes e bibliotecas de software obsoletos ou inseguros podem permitir que o dispositivo fique comprometido. A personalização insegura das plataformas do sistema operativo e o uso de software ou o uso de componentes de hardware de terceiros.

6 - Proteção de privacidade insuficiente:

Informações pessoais de utilizadores armazenadas no dispositivo ou no ecossistema que são usadas de maneira insegura, imprópria ou sem permissão.

7 - Transferência e armazenamento de dados inseguros:

A ausência de criptografia ou o controlo de acesso a dados confidenciais em qualquer parte da rede, incluindo quando este se encontra desligado, em comunicação ou durante o processamento.

8 - Falta de gestão de equipamentos:

A falta de suporte de segurança em equipamentos colocados em produção, incluindo a gestão de ativos, gestão de atualizações, desativação segura e monitorização de sistemas.

9 - Configurações padrão inseguras:

Os equipamentos ou os sistemas são fornecidos com configurações padrão inseguras onde existe falta de capacidade de tornar o sistema mais seguro, com restrições para modificar as configurações.

10 - Falta de bloqueios físicos:

A falta de medidas de proteção física, permite que invasores obtenham informações confidenciais que possam ajudar num futuro ataque remoto ou consigam assumir o controlo do dispositivo local.

Após analisar a lista do Top 10 dos riscos fornecida para OWASP procedeu-se á respetiva interpretação, constatando que a gestão de riscos ajuda as empresas e as organizações a entender o que é o risco, o que está em risco e quais as ações para os mitigar. Se existirem ações que não são adequadas então não serão necessárias ações complementares para gerir o nível de risco.

A Lei 46/2018 de 13 de agosto [70] obriga à adoção de um conjunto de medidas que garantam a resiliência e uma mitigação do risco de ataques em conjunto com a capacidade de responder adequadamente à reposição dos níveis de serviço num espaço de tempo definido e aceitável.

De realçar que os mais variadíssimos equipamentos IoT necessitam de transmitir, armazenar e processar dados, contudo esta transmissão pode tornar-se problemática. É fundamental garantir uma transmissão de dados de forma encriptada ou com mecanismos de autenticação eficazes.

Esta recolha massiva de dados permite uma fácil monitorização das atividades de cada equipamento, utilizando sistemas cada vez mais sofisticados, existindo alguns dotados de capacidades de adaptação e de aprendizagem.

Os dados podem ser recolhidos de forma massiva com uso de scripts tornando estas tarefas simples e automatizadas. Os dados podem ser posteriormente guardados em base de dados para serem facilmente acedidos e consultados.

Com o acesso indiscriminado à internet, os dados são utilizados em vários sites e nos próprios equipamentos, sendo que o utilizador na maioria dos casos não tem uma noção clara do uso que é dado aos seus dados. Estas preocupações estão a ser abordadas pelo NIST num documento que ainda se encontra em rascunho[71] e em fase de recolha de informações.

Os equipamentos IoT ao produzirem informações confidenciais deveriam garantir quem tem acesso a esta informação, encriptando os dados de forma a camuflar os dados que são transmitidos.

Para se garantir a confidencialidade é necessário utilizar mecanismos de criptografia modernos e robustos. Estes algoritmos devem ser públicos, sendo apenas a chave de encriptação secreta. A gestão das chaves de encriptação é um risco e uma tarefa complexa e crítica, uma vez que o tempo de exposição da chave é grande não existindo uma rotatividade constante ou uma alteração frequente destas.

Os equipamentos que não estejam dotados de um sistema de confiança são um potencial risco. A troca de credenciais entre um serviço ou uma aplicação devem ser acauteladas e o relacionamento entre estas aplicações não deverá levantar suspeitas.

O controlo de acessos em equipamentos IoT é também um grande desafio por parte dos fabricantes dado existir uma grande abertura por parte destes para que qualquer equipamento se interligue, no entanto não existem medidas que tratem os direitos dos acessos concedidos a outros aparelhos IoT. Este risco deverá estar presente nas equipas de TI locais uma vez que

a grande maioria dos equipamentos IoT tem pouco ou nenhum armazenamento interno, sendo difícil fazer uma análise posterior aos logs gerados por si.

A comunicação realizada por middleware entre os equipamentos IoT é outro risco e um problema que deverá ser tido em consideração. Os dados transferidos ou emitidos não possuem proteções, tornando difícil o crescimento da tecnologia em termos de segurança e privacidade.

As redes programáveis também têm crescido e a sua expansão tem sido exponencial, no entanto é necessário acautelar o seu uso evitando instalações de programas ou scripts que poderão ter aplicações ou rotinas que efetuem um conjunto de ações mal-intencionadas.

O termo *botnet* está associado a um robot ligado á internet que tem a finalidade de fazer tarefas repetidas consecutivamente. Este tipo de ataque é utilizado para ataques de negação de serviço, sendo que o espectro de ação é muito amplo. Os botnets podem comprometer computadores, cuja segurança foi violada e o controlo cedido a terceiros.

Já o simples facto de desligar equipamentos da rede pode não ser solução suficiente para a segurança de alguns ecossistemas. A principal característica dos objetos IoT está na capacidade de transmitir e receber informação, no entanto para isto não necessitam de uma ligação à internet. Em alguns dos casos os equipamentos armazenam os dados e retransmitem a informação quando se encontram em modo online novamente.

Atualmente os equipamentos IoT são responsáveis por gerar muita informação, uma vez que estão sempre a recolher e a interpretar os dados nos diversos sensores a cada segundo ou nano segundo. A necessidade de fornecer mecanismos que permitam a análise de um grande volume de informação (bigdata) de forma a extrair dados significativos é um desafio, sendo difícil a sua leitura e o seu armazenamento devido á quantidade de informação gerada.

O malware é um tipo de ameaça que poderá alterar dados de um dispositivo e comprometer o diagnóstico, sendo destinado a realizar ações não autorizadas, podendo causar danos no equipamento ou na rede

Com o crescimento do número de objetos, dispositivos, ou equipamentos com interfaces, serviços e capacidades próprias, a interoperabilidade torna-se um elemento fundamental para a integração entre todos.

Uma rede interoperável torna possível o uso de padrões técnicos partilhados, possibilitando uma troca fácil de dados e informação.

Assim, de forma a todos os equipamentos ligados se comunicarem de forma padronizada mitigando o risco, é fulcral que os desenvolvedores adotem uma linguagem que possibilite uma harmonia entre os demais sistemas ligados.

No que diz respeito aos protocolos de comunicação, o protocolo HL7 é o protocolo privilegiado na área da saúde. O HL7 já conta com uma grande disseminação mundial, no entanto ainda não está generalizado que todos os equipamentos que difundem dados de saúde utilizem este protocolo para envio e recolha de mensagens.

Os equipamentos IoT estão muito expostos na rede a ataques, transmitem os dados sem fios, em um intervalo temporal definido, o que facilita a implementação de ataques de falsificação. A transmissão e o processamento de dados enfrentam ainda todas as questões de segurança já conhecidas, existentes na rede TCP/IP.

As equipas de TI das unidades de saúde devem estar sensibilizadas para os variados pontos de entrada que existem na rede. Cada vez mais existem variadíssimos equipamentos ligados em rede, sendo que todos eles têm vulnerabilidades de segurança no software, hardware e firmware usado por esses equipamentos.

2.7. Vulnerabilidades do IoT

A enorme proliferação de equipamentos IoT e a falta de segurança robusta nestes equipamentos representam uma ameaça crescente à segurança e à privacidade dos indivíduos e empresas que os utilizam. Os equipamentos IoT são feitos de uma panóplia cada vez maior de software e hardware, levando a uma significativa complexidade, que dificulta a implementação de controlos de segurança. Assim é importante que a segurança seja abordada ponto a ponto, já que tudo está interligado entre si.

A IETF-Internet Engineering Task Force no RFC 2828 [72] define “vulnerability” como “uma falha ou uma fraqueza no desenho do sistema, na sua implementação ou operação que pode ser explorada de forma a violar a política de segurança dos sistemas.”

Entre os diversos aspetos sobre a segurança de IoT o projeto OWASP [73] elenca as 10 principais vulnerabilidades do IoT, que devem ser a base para avaliação nas organizações ao desenvolverem ou implementarem estes projetos, nomeadamente:

1. Segurança física dos objetos/equipamentos inteligentes;
2. Software/firmware vulnerável;
3. Falta de criptografia e verificação da integridade dos dados;
4. Configuração insuficiente na segurança dos objetos;
5. Autenticação/autorização insuficiente nos equipamentos;
6. Serviços de redes vulneráveis (privadas ou Internet);
7. Interface da cloud vulnerável;
8. Interface de gestão dos IoT vulneráveis;
9. Interface móvel dos IoT vulneráveis;
10. Privacidade de dados dos utilizadores de IoT.

A existência ou a identificação de uma vulnerabilidade não causa danos por si só. É necessário a existência de uma ameaça que explore essa vulnerabilidade para que o equipamento seja comprometido.

As unidades de saúde devem estar alerta e cientes das ameaças para os vários pontos de entrada que existem na rede. São centenas de equipamentos interligados, cada um deles portador de vulnerabilidades tanto no seu hardware como no seu software.

Os protocolos que possibilitam o acesso remoto são normalmente os primeiros a serem testados quando se procuram vulnerabilidades. Estes tipo de falha é um alvo muito testado e procurado por hackers ou cibercriminosos uma vez que são muitas vezes mal configurados com palavras passe fracas, ou palavras passe padrão que se encontram expostas na internet. O botnet Mirai [74] é um exemplo de que este tipo de ataques está presente no nosso dia-a-dia.

Os testes de penetração ou os pentest, são efetuados para validar as vulnerabilidades existentes em um determinado equipamento, “identificando o que um atacante consegue ganhar após um ciberataque bem sucedido” [75]. Este tipo de teste é muito útil uma vez que é possível ter uma visão ampla das vulnerabilidades que determinado equipamento tem, podendo assim tomar-se medidas para acautelar este tipo de vulnerabilidade comum já identificada.

A exploração de vulnerabilidades pode ser feita através da tentativa da violação do sistema de autenticação. Este tipo de exploração é feito por norma com ataques de bruteforce, de

forma a tentar obter acesso ás credenciais do dispositivo obtendo mais privilégios para controlar o equipamento.

A maioria dos equipamentos não tem a melhor abordagem de segurança de rede, não exigindo senha para autenticação nem se preocupam com complexidade das mesmas. São equipamentos que na sua génese são programados com passwords fracas ou previsíveis, e o manual está disponível no site do fabricante para consulta onde se pode facilmente retirar a password por defeito. Os exemplos mais comuns são o típico *admin* ou o 12345.

Existem várias ferramentas gratuitas que automatizam este tipo de ataques ao sistema de autenticação dos equipamentos, mais propriamente aos portais web onde tentam o acesso seja por brute force, ou por passwords padrão. Este tipo de ataque pode ser feito por exemplo com softwares como o Hydra, Medusa ou NCrack, presentes na distribuição Kali Linux.

Outra vulnerabilidade a ter em conta centra-se nos mecanismos adequados de proteção dos equipamentos que na maioria das vezes não sofrem atualizações de segurança regulares ou periódicas, tratando-se de equipamentos com configurações padrão consideradas inseguras.

A transferência e o armazenamento de dados não é na maioria dos casos encriptado, pelo que pode ser fácil intercetar os dados transmitidos. Os equipamentos mais pequenos podem ser roubados, sendo analisado os dados fora do contexto onde se encontram.

A maioria dos fabricantes deixa portos abertos (backdoors) para poder prestar pedidos de suporte se necessário. As empresas e fabricantes dos equipamentos IoT também querem conhecer melhor os hábitos dos seus consumidores, e qual o tipo de uso que os equipamentos têm, de forma a melhorar as funcionalidades que dispõem, no entanto isto gera muita informação que deverá ser tratada (BIG DATA). É fulcral perceber que telemetria está a ser enviada nos equipamentos, e quais os portos abertos, bloqueando nas firewalls de perímetro o acesso a estes equipamentos e a estas portas.

Um dispositivo IoT é uma combinação de hardware e software que comunicam entre sim através do firmware. O firmware original pode ser modificado por um firmware malicioso que poderá alterar a forma de funcionamento do equipamento. A análise do firmware é a principal forma de descobrir outras vulnerabilidades.

O firmware está quase sempre presente na página do fabricante, pelo que o risco de explorar este código fonte é elevado, não sendo necessário o acesso ao dispositivo para explorar uma

vulnerabilidade. Este tipo de ação é uma vulnerabilidade que não afeta diariamente a segurança do dispositivo, no entanto fornece informações que poderão ser usadas para explorar outras vulnerabilidades.

A maioria dos equipamentos IoT está dotado de uma aplicação web acessível através da internet, para gestão, configuração ou monitorização do equipamento. Estas páginas são alvo de ataques contantes, seja por SQL injection [76], onde esta vulnerabilidade permite correr código SQL de forma não autorizada com o intuído de ler ou alterar dados de uma base de dados, de forma a executar código não autorizado. Outra vulnerabilidade conhecida para comprometer as plataformas web é o CROSS-Site Scripting (XSS). Esta vulnerabilidade consiste na execução de código malicioso através do browser quando é acedido. Este código pode ser utilizado com vários fins e proveitos sendo que a o principal objetivo foca-se na obtenção dos cookies de autenticação para escalar privilégios.

A adoção lenta de padrões [77] é outro tema a ter em consideração, uma vez que os equipamentos IoT se regem todos pelos mesmos standards, ficando assim mais difícil gerir todos os equipamentos, uma vez que cada equipamento tem o seu método de autenticação, o seu método de armazenamento, comunicação e transferência de dados diferente entre si.

Em suma, a maioria dos equipamentos IoT tem pouca energia, estão dotados de um microcontrolador de baixo custo e a memória que possuem é limitada. No entanto, estas características tornaram esta mudança dos controladores de IoT ainda mais desafiadora, já que os protocolos de internet existentes normalmente não são projetados para este tipo de equipamentos com outras funcionalidades incorporadas.

Já a classificação das vulnerabilidades é fundamental para atribuir um valor ao seu nível de risco. Esta classificação poderá ser subjetiva, fruto da interpretação dada aos resultados obtidos. Existem standards para classificar o risco de vulnerabilidades, sendo esta compreendida em valores[78] de 0 a 10.

2.8.Síntese

Neste capítulo foi efetuado um levantamento do conhecimento científico na área dos equipamentos IoT, na qual se insere este trabalho. Pretendeu-se de uma forma abrangente dar a conhecer os conceitos que se consideram imprescindíveis para conhecer o funcionamento desta tecnologia

Na primeira parte do capítulo, para além de um breve enquadramento histórico, foram abordados e verificados quais os tipos de comunicação que este tipo de tecnologia utiliza. Foram também verificados quais os protocolos mais usuais assim como os protolocos de comunicação mais utilizados, nomeadamente o MQTT, CoAP e o HTTP.

Como se trata de um trabalho direcionado para lidar com informações clínicas ou de saúde, também são apresentadas as normas de comunicação standards mais enraizadas neste setor, são elas o HL7, Dicom e OpenEHR.

Após esta análise mais científica tornou-se imprescindível analisar quais os tipos de ataques e os tipos de ameaça a que estes tipos de equipamentos IoT estão propensos, analisando também os variados riscos e vulnerabilidades.

3. Caracterização de equipamentos IoT

Os equipamentos IoT presentes nas unidades de saúde, são cada vez mais equipamentos que permanecem ligados à rede, interligando-se entre si e a cada instante geram informação constante. Estes equipamentos são considerados objetos inteligentes, robustos, com a capacidade de criarem novas redes independentes que operam com as suas próprias infraestruturas e ou protocolos.

Este capítulo aborda os diversos equipamentos IoT que se podem encontrar em unidades de saúde e serão abordados os tipos de ataque mais comuns a que cada equipamento está sujeito.

São equipamentos que podem estar ativos na rede a enviar e a receber informação, ou podem ser passivos, a armazenar a informação no sensor para uma posterior leitura. Uma das principais características destes equipamentos é o fornecimento de dados quando e onde for necessário, preenchendo a falha que existe entre o mundo web e o mundo real isento de falhas na transcrição pela mão humana.

A utilização de determinados equipamentos em unidades de saúde ou em ambientes hospitalares visam a recolher informações de forma precisa e sem intervenção do ser humano, o qual pode vir a cometer uma falha na leitura ou na recolha desses mesmo dados. Os dados também poderão ser recolhidos com maior fiabilidade, a horas precisas e com a mesma cadência ao longo do dia, libertando os profissionais de saúde para outras tarefas na prestação de cuidados de saúde.

São equipamentos que na sua generalidade estão ligados á rede da instituição ou da unidade de saúde, pelo que os equipamentos apresentados não são todos de cariz médico, são abordados alguns equipamentos que são considerados problemáticos como é o caso de uma impressora, por exemplo, equipamento presente em qualquer modelo de negócio, no entanto pode ser o foco de entrada para um ataque como irá ser abordado e ganha o título de IoT a partir do momento que é ligado à rede.

Elencam-se de seguida alguns exemplos de equipamentos que poderão estar ligados á rede numa unidade de saúde:

3.1.Equipamentos clínicos

Em unidades de saúde, a panóplia de equipamentos ligada á rede é muito diversificada, no entanto, no âmbito desta dissertação foram identificados os principais equipamentos clínicos que se encontravam ligados na rede no momento.

Após a identificação destes equipamentos clínicos, foram abordados quais poderiam ser os riscos e as vulnerabilidades mais comuns em cada equipamentos, com base no estado da arte anteriormente analisado.

3.1.1. Dispensadores de medicação

Os dispensadores de medicação são utilizados nas unidades de saúde com farmácia hospitalar integrada. São equipamentos que na sua maioria detêm um sistema operativo descontinuado e/ou obsoleto, que integram diversos equipamentos mecânicos, entre eles gavetas que na sua maioria foram concebidos para funcionarem com um determinado sistema operativo, como é o caso do Windows XP que deixou de ser suportado em fevereiro de 2015, e o Windows 7 deixará de ter suporte em janeiro de 2020. Apesar de funcionarem corretamente e cumprirem com a função para o qual foram concebidos, não existe uma sensibilização por parte dos administradores para procederem a um novo investimento para aquisição de equipamentos mais recentes.

Existem por exemplo equipamentos com Windows XP com controladores de hardware que também deixaram de ter suporte com outras versões de Windows mais atuais, inviabilizando assim o uso do equipamento, independentemente de atualização do sistema operativo. É perentório que os fabricantes trabalhem lado a lado para possibilitarem a continuidade de negócio, acompanhado a evolução de todo o ecossistema.

Estes equipamentos, são autênticos robots que possibilitam a triagem, a separação e a rotulagem de medicação corretamente, para dispensa à cabeceira do utente.

São equipamentos que estão suscetíveis a ataques de ransomware, e por consequência à negação de serviço, ou à manipulação da informação, podendo causar efeitos negativos no tratamento do doente.

Caso o equipamento fique inoperacional, a garantia da distribuição da medicação atempadamente fica comprometida, sendo necessário reforçar as equipas para fazer a distribuição dos fármacos e a respetiva etiquetagem.

Se o equipamento for atacado e se o cibercriminoso proceder à alteração da medicação por cama este poderá comprometer a segurança do utente.

Os dados recolhidos podem também ser capturados e vendidos no mercado negro, expondo assim o tratamento que cada utente teve direito, identificado por exemplo se um dado utente tem algum distúrbio psíquico em função do fármaco que lhe foi administrado, ou alguma doença grave que inviabilize um crédito ou um seguro de vida.

São equipamentos que ajudam muito os profissionais de saúde nas suas tarefas diárias, pelo que deverão ser tomadas medidas de segurança para garantir que o equipamento não fique exposto na rede a ataques conhecidos.

3.1.2. Estações de aquisição de imagem

As estações de aquisição de imagem são utilizadas para diagnosticar um elevado leque de doenças, e permitem visualizar em tempo real diversas partes internas do organismo, capturando imagens para posterior análise e relatório.

Na sua maioria, todos estes equipamentos integram com um PACS (Sistema de Comunicação e Arquivo de Imagens) e estão interligados por rede utilizando o protocolo TCP/IP para comunicar entre si enviando as imagens com o protocolo DICOM.

Estes equipamentos estão suscetíveis a ataques de negação de serviço, ou a ataques de man-in-the-middle, sendo possível intercetar as imagens capturadas, e arquivá-las por exemplo em nome de outro utente, ou simplesmente descartá-las. Este tipo de ação pode levar a diagnósticos errados por parte das equipas médicas, causando efeitos nefastos ao utente sem que ninguém se aperceba do que ocorreu. É uma prática de terrorismo clínico que pode ser utilizada para causar ausência de cuidados, ou cuidados errados.

São equipamentos muito caros, sujeitos a concursos públicos de aquisição, onde são efetuados contratos de manutenção para garantir a disponibilidade do equipamento. No entanto os updates de firmware nem sempre são contemplados, pelo que se deverá ter especial atenção ao que é contratualizado.

3.1.3. Monitores de sinais vitais

Os monitores de sinais vitais tal como o nome indicam, monitorizam os sinais vitais de um utente, nomeadamente os batimentos cardíacos, a tensão arterial, a temperatura, e a

oxigenação. Existem monitores que fazem também um ECG (eletrocardiograma), um exame de rotina que avalia o ritmo dos batimentos cardíacos.

Estes monitores emitem alertas para auxiliar as equipas de cuidados médicos, para uma rápida atuação em caso de ausência de sinais vitais.

A principal vulnerabilidade deste equipamento foca-se na ausência de autenticação do protocolo que utiliza na comunicação, podendo ser possível emular informações falsas ás equipas médicas, disponibilizando valores diferentes dos reais comprometendo a saúde e o bem estar do paciente.

É fulcral analisar se os dados transmitidos por este tipo de equipamentos, é encriptado. Existem relatos [79] de equipamentos que transmitem os dados em cleartext[3]. Os dados extraídos destes equipamentos podem assim ser capturados e colocados á venda em mercados negros, apresentando um historial clínico de um determinado utente, inviabilizando a estes por exemplo o acesso a seguros de saúde ou a créditos na banca, caso estas empresas tenham conhecimento prévio dos futuros clientes.

3.1.4. Bombas de perfusão

As bombas de perfusão, permitem injetar líquidos no corpo humano, nomeadamente fármacos ou nutrientes, com um preciso controlo de fluxo e de volume nas vias venosas ou arteriais.

Este tipo de equipamento auxilia as equipas médicas ao administrar quantidades certas e precisos e com ciclos pré-definidos de medicação, evitando a deslocação de um médico ou de um enfermeiro constantemente junto do doente para esta tarefa. Apesar das suas vantagens estes equipamentos têm alguns interfaces de comunicação, nomeadamente, portas USB e portas de rede para configuração e monitorização nos mais variados cenários.

O acesso á bomba também pode ser feito por um portal web, com passwords fracas ou por defeito, onde pode ser definido os fluxos e as quantidades que são injetadas. A comunicação não é criptografada pelo que poderá ser possível capturar o tráfego.

[3] Termo utilizado em informática que define que não existe encriptação ou que é possível ler o que é transmitido.

São equipamentos que não costumam receber updates de firmware automáticos, pelo que poderão ter as suas fragilidades já conhecidas a descoberto.

O acesso indevido por pessoas mal-intencionadas a este tipo de equipamentos pode ser utilizado para causar prejuízo na vida do utente, ou para recolha de informação e posterior comércio da informação em mercados negros.

3.1.5. Bombas de insulina

As bombas de insulina são utilizadas diariamente por diabéticos que entregam o seu bem-estar a estes equipamentos ficando assim despreocupados com a dosagem de insulina que lhes é administrada sendo esta responsabilidade incutida ao equipamento.

São equipamentos que já contam com vulnerabilidades conhecidas [23], nomeadamente ao nível da comunicação sem fios uma vez que não dispõem de autenticação nem autorização.

Assim devem ser tomadas medidas para evitar que estes equipamentos coloquem em risco vidas humanas, seguindo as indicações do fabricante, atualizando para os firmware mais atuais quando estes são disponibilizados.

Estes equipamentos são transportados pelos utentes, para dentro e para fora das unidades de saúde, pelo que se tornam um potencial risco, uma vez que pode existir utentes com ideias de violar a segurança da informação, e injetar neste tipo de equipamentos vírus ou malware que poderá ter impacto na rede da unidade de saúde.

3.1.6. Vídeo-Cápsula

A vídeo-cápsula utilizada para diagnosticar problemas do trato digestivo, examina cada detalhe percorrendo todo o trajeto dos alimentos em todo o seu percurso digestivo.

A cápsula está dotada de uma camara fotográfica e de um flash, e vai capturando fotos a cada instante. O utente por norma traz um recetor à cintura onde as imagens vão ser recolhidas.

Estas cápsulas por norma não trazem métodos de autenticação, sendo possível intercetar as imagens enviadas para o recetor. Apesar de não causar grande impacto, este tipo de ataques pode levar á repetição do exame causando prejuízo no utente ao não ter a doença diagnosticada atempadamente.

3.1.7. Esfigmomanómetros

Os esfigmomanómetros são aparelhos utilizados na sua génese para verificar a tensão arterial e a pulsação arterial do utente. São equipamentos de uso pontual, pelo que não são utilizados para fazer uma monitorização continua. Alguns equipamentos deste tipo permitem a ligação á rede para descarregar as leituras efetuadas.

São equipamentos que podem sofrer de ataque man-in-the-middle, pelo que os dados anexados a um processo clínico podem não ser os dados realmente obtidos, levando as equipas médicas a um diagnóstico errado. A não atualização deste tipo de equipamentos também pode comprometer outros equipamentos de rede, podendo este ser utilizado para explorar falhas ou vulnerabilidades presentes na infraestrutura da unidade de saúde.

São equipamentos que têm portas rs232 ou portas usb disponíveis que não são utilizadas, pelo que a presença deste tipo de ligações pode ser explorada para obter outro tipo de privilégios.

3.1.8. Pacemaker

O pacemaker é um dispositivo médico que tem como objetivo regular os batimentos cardíacos de um doente.

São equipamentos que possibilitam acesso por intermédio de um aparelho intermédio denominado MICS (Medical Implant Communication Service). Este MICS é ligado ao computador onde possibilita fazer um check-up ao pacemaker, assim como configurar a cadência ou o ritmo a incutir no coração.

São equipamentos que necessitam de uma intervenção cuidada e cautelosa para implementação, uma vez que é necessária uma cirurgia evasiva. É um equipamento fulcral á vida humana e que pode levar á morte se fôr mal configurado.

Um pacemaker ao ficar comprometido ao nível de segurança tem como principal risco levar o paciente á morte, ou sob o risco do paciente ter que ser sujeito a nova cirurgia para remover o equipamento em questão.

3.1.9. Monitor de glicose

Os diabéticos, necessitam controlar os níveis de glicose regularmente para não sofrerem nenhuma hipoglicémia ou hiperglicemia. Estas duas patologias podem ser fatais se os valores de glicémia forem substancialmente baixos, ou substancialmente altos respetivamente.

Assim, com os monitores de glicose, os diabéticos conseguem equilibrar os níveis de glicose, podendo administrar mais ou menos insulina, em função dos valores apresentados.

Existem equipamentos que carecem de uma lanceta que perfura o dedo para obter uma gotícula de sangue para análise.

Estes equipamentos recolhem os dados que posteriormente podem ser analisados por um profissional de saúde em gráfico ou em tabelas no computador.

Existem também equipamentos (por exemplo o FreeStyle Libre) que prescindem da lanceta, sendo apenas necessário encostar o equipamento ao braço para efetuar a leitura.

O principal risco da utilização deste equipamento está relacionado com a alteração de valores, e de uma possível sobredosagem na dose de insulina a administrar. Ao ligar estes equipamentos à rede é fundamental que os computadores locais tenham políticas de segurança bem definidas e as últimas atualizações dos antivírus instaladas de forma a mitigar uma possível intrusão, ou contaminação de malware que poderá ter efeitos em toda a infraestrutura.

3.2. Equipamentos de suporte e periféricos

Uma unidade de saúde tem presente na sua infraestrutura de rede variadíssimos equipamentos de suporte e outros periféricos que possibilitam funcionalidades de logística, de monitorização ou de alarmística, que não são exclusivos de uso clínico.

Este tipo de equipamentos ajuda a monitorizar outros sensores para garantir o bom funcionamento do modelo de negócio da unidades de saúde. São equipamentos que não lidam diretamente com dados clínicos, no entanto são fundamentais para a continuidade do negócio.

São equipamentos que ganham o estatuto de IoT a partir do momento que são ligados à rede, partilhando informações que podem ser extraídos e analisados. São também equipamentos que são utilizados no dia-a-dia como é o caso das impressoras, das televisões ou dos frigoríficos. Equipamentos banais que na sua génese foram comprados com o propósito a que se destinam, mas que possibilitam outro tipo de funcionalidades, colocando em risco a instituição de saúde.

3.2.1. Pulseiras de identificação de bebés

O despacho n.º 20730/2008 do decreto de lei nº 152 de 7 de agosto de 2008 veio obrigar as unidades de saúde a utilizarem pulseiras nos recém-nascidos de forma a evitar o rapto e a troca de crianças.

Estas tags ou pulseiras garantem que um determinado bebé corresponde a uma determinada mãe sendo possível localizar o bebé dentro do edifício com recurso á triangulação do sinal da rede wi-fi.

Caso a tag se aproxime de uma zona de saída não autorizada o sistema gera um alarme automático com a indicação do bebé que se aproximou dessa zona, despoletando medidas preventivas, nomeadamente o fecho de portas, bloqueio de elevadores, sinalização luminosa e acústica.

Se o sistema for violado, será possível iludir o sistema criando a ilusão que o bebé se encontra em determinada zona, quando na realidade poderá já estar fora do edifício.

De salientar que os routers utilizados poderão ter as credenciais de acesso por defeito ou nunca terem sofrido atualizações de firmware.

3.2.2. Sensores de temperatura

Os sensores de temperatura, recolhem com alta precisão os valores de temperatura, humidade e ou a pressão atmosférica de um dado local. Nas unidades de saúde são muito utilizados para garantir a temperatura correta no acondicionamento da medicação.

A alteração forçada destes valores pode levar ao prejuízo em milhares de euros em medicação, ou poderá ter efeitos negativos se o sensor indicar uma temperatura falsa, mas na realidade estiver a debitar outra.

Estes sensores geralmente funcionam em paralelo com os sistemas de arrefecimento (chiler ou ar condicionado), pelo que a atmosfera será refrigerada ou aquecida em função da leitura que for efetuada pelo sensor de temperatura.

3.2.3. Sensores de dióxido de carbono

Os sensores de dióxido de carbono permitem monitorizar um determinado lugar, analisando a qualidade do ar permanentemente, verificando se existe a presença de dióxido de carbono (CO2).

Estes equipamentos permitem a ligação á rede, onde é possível configurar parâmetros e extrair dados para estatística.

Existe ainda a possibilidade de configurar os equipamentos para despoletar uma ação após um determinado valor. A título de exemplo, é possível abrir janelas automáticas e ligar os extratores de ar quando se verificar um determinado valor elevado de CO2.

O maior risco associado a este equipamento poderá estar na captura dos dados, e informar posteriormente os variados sensores de valor errados, falsificando a leitura correta.

É fundamental atualizar o equipamento com os últimos updates de firmware e proceder à alteração das passwords por defeito para passwords com maior grau de complexidade e passwords diferentes de outros equipamentos. Uma pessoa mal-intencionada pode tentar o controlo indevido sobre um equipamento mais pequeno, sem tanto impacto e explorar a utilização dessa password em outro equipamento da rede.

3.2.4. Portas automáticas

As portas automáticas, tem um dispositivo de comunicação que permite o seu controlo através de um servidor web ligado á rede por TCP, onde é percetível o histórico de incidências (aberturas/fechos), trincos, e inclusive é possível controlar o horário de funcionamento da porta.

Atualmente a facilidade com que se abre e fecha uma porta de forma remota poderá trazer riscos para a segurança do edifício, uma vez que os servidores que controlam as portas podem ser atacados por pessoas mal-intencionadas, proporcionando o roubo de bens ou vedando o acesso a pessoas ao edifício.

É fulcral atribuir estes acessos apenas a funcionários credenciados para o efeito, sensibilizando-os para os ataques de engenharia social que poderão ser levados a cabo para ter acesso á instituição.

3.2.5. UPS (Uninterruptible Power Supply)

As UPS ou as fontes de corrente estabilizada, garantem que um aparelho não fica com ausência de corrente elétrica, assegurando que a corrente que lhe chega é estabilizada e isenta de tensões anormais.

Estes equipamentos permitem a ligação a um webserver onde é possível verificar que energia está a ser debitada em cada saída, verificar os logs de interrupção de serviço, e em alguns equipamentos é possível fazer um reboot remoto.

Este tipo de equipamento ganha o estatuto de IoT a partir do momento que é ligado á rede, para ser monitorizado. É com esta ligação de rede que passa a ser um equipamento vulnerável, dado não possuir autenticação cifrada é possível a pessoas mal-intencionadas desligarem equipamentos de cariz fulcral na instituição indevidamente ou propositadamente.

3.2.6. Impressoras

Apesar da desmaterialização do papel que se tem vindo a fazer sentir, as impressoras ainda são um equipamento presente e fundamental nas unidades de saúde. O principal risco destes equipamentos quando ligados á rede por TCP/IP foca-se na disponibilização do webservice, onde poderá ser possível capturar os documentos da fila de trabalho e ter assim acesso a documentos de cariz confidencial.

Cada vez mais se imprime menos, no entanto o risco de encontrar uma impressora vulnerável com um firmware desatualizado é grande, pelo que poderá ser utilizado por pessoas mal-intencionadas para adquirir informação preciosa para ajudar em um ataque de engenharia social.

As impressoras também podem ser utilizadas para aceder a outros equipamentos da rede, ou seja, podem facilmente tornar-se a "máquina de salto" para ajudar a entrar na rede, isto é, algumas impressoras têm a ligação Wi-fi aberta, que por sua vez têm uma ligação direta ou indireta a um computador. Assim torna-se perentório que as unidades de saúde olhem para as impressoras como um equipamento a ter em conta ao nível da cibersegurança.

Em agosto de 2018, a HP. corrigiu centenas de modelos a jato de tinta vulneráveis a duas falhas de execução remota de código disponibilizando as respetivas falhas na lista de vulnerabilidades comuns (CVE-2018-5924, CVE-2018-5925).

Um estudo patrocinado pela HP[80] constatou também que 56% dos entrevistados, alegam não ter qualquer tipo de política de segurança para as impressoras ligadas à rede nas organizações.

3.2.7. Controladores de Autómatos

Os demais variadíssimos autómatos utilizados para controlar por exemplo bombas de água, elevadores, geradores, quadros elétricos, entre outros, são equipamentos que se encontram ligados á rede na sua maioria por via de um computador.

Os mais vulneráveis, são na sua génese equipamentos com alguma idade, colocados em produção aquando a inauguração dos edifícios e cuja a sua modernização estagnou, no entanto desempenham a função para o qual foram programados, não havendo necessidade de efetuar atualizações sob risco de este se tornar inoperacional.

Apesar da sensibilização das equipas de tecnologias de informação, estes autómatos ainda se encontram nas redes e são um foco que deve ser sanado.

Os autómatos mais recentes já permitem a atualização de firmware e não estão dependentes de um computador com aplicações proprietárias para servir de interface na ligação.

Os principais riscos focam-se na negação de serviço, e no impacto que podem causar no negócio.

3.2.8. Controlos de Acesso

Os controlos de acesso permitem abrir e fechar portas, assim como permitem fazer a gestão de pessoal, permitindo efetuar o controlo das horas a que iniciaram e terminaram a sua produção.

São sistemas que apesar de funcionarem com a impressão digital, têm sempre um método alternativo para não se tornarem inoperacionais. A título de exemplo existem profissionais com a impressão digital muito ténue que não conseguem fazer a sua leitura nestes equipamentos. Existe também a possibilidade de uma pessoa ter um acidente e ficar com os dedos registados na base de dados inoperacionais. Assim, para colmatar estas falhas ou contornar estas dificuldades os fabricantes permitem registar utilizadores com acesso a um pin ou um código, evitando assim a inviabilização do equipamento.

Estes equipamentos por norma geral também tem um utilizador por defeito para possibilitarem em caso de necessidade o acesso a forças de segurança (exemplo: bombeiros e polícia) evitando que danifiquem a porta em questão.

O acesso por pessoas mal-intencionadas a este equipamento, comprometendo a integridade, permite a indisponibilidade de serviço, que se poderá traduzir numa ação catastrófica quando se pretende controlar o acesso a uma unidade de saúde. Este tipo de instituições têm por vezes mais de mil funcionários que poderão ficar impossibilitados de entrar no edifício.

A captura dos dados destes funcionários também pode ser usada para realizar ataques de engenharia social, uma vez que é possível perceber as rotinas dos funcionários e os fluxos de acesso.

3.2.9. Quiosques de pagamento automático

Os quiosques de pagamento são utilizados para tornar os edifícios mais práticos e fluidos, reduzem o tempo de espera aos utentes uma vez que possibilitam ao utente efetuar pagamentos e admissões autonomamente sem necessidade de intervenção de um funcionário da instituição.

Estes equipamentos são equipados com dispensadores de senhas e um cofre mealheiro, ou um terminal de multibanco, onde é possível efetuar pagamentos, a admissão a uma determinada consulta e pagar as taxas moderadoras em dívida.

Estes quiosques, na realidade são vulgares computadores que dispõem de diversos periféricos instalados para funcionarem de forma muito simples e intuitiva por intermédio de um touchscreen. Ao tratarem-se de computadores, são equipamentos ligados á rede e suscetíveis a ataques.

A negação de serviço e o pagamento indevido de taxas moderadoras são exemplos de ataques que podem ocorrer nestes equipamentos. É perentório que estejam atualizados, no entanto, dado tratar-se de um conjunto de periféricos, nem sempre é fácil garantir o funcionamento dos diversos periféricos instalados com as diferentes atualizações de sistema.

3.2.10. Central telefónica

A central telefónica de uma unidade de saúde é um equipamento muito importante e fundamental para a continuidade do negócio de uma unidade de saúde. Existem centrais telefónicas analógicas e digitais.

As centrais telefónicas têm um teclado que permite o interface entre o computador e o telefone, sendo possível reencaminhar chamadas, gravar, colocar em espera, entre outras funcionalidades que as consolas permitem de forma muito fácil e intuitiva para o utilizador.

Como principal ameaça, estes equipamentos de serviço estão suscetíveis à negação de serviço ou á captura de informação de acesso confidencial ou restrito, sendo fundamental as atualizações de firmware e do sistema operativo.

3.2.11. SmartTV

As televisões inteligentes estão um pouco distribuídas pelas diversas unidades de saúde quer em salas de espera, em salas de reunião ou em gabinetes de consulta.

São televisões que são ligadas á rede utilizadas para passar conteúdos de streaming de portais online, nomeadamente visualização de vídeos ou músicas do youtube.

Estes equipamentos são muito vulneráveis uma vez que não sofrem atualizações automáticas de firmware.

São esquipamentos que podem ser acedidos remotamente e a partir deles ter acesso á rede e por consequente a outros equipamentos da rede.

3.2.12. Câmaras de videovigilância ou webcams

As câmaras de videovigilância ou as webcams são equipamentos que possibilitam a vigilância de pessoas, bens ou de um determinado local em tempo real, podendo ser captado áudio e vídeo no presente momento. Alguns equipamentos estão dotados de motor, que são possíveis controlar remotamente, possibilitando assim alargar o espectro de visão da câmara, alcançando outros locais com mais detalhe. São equipamentos que na sua maioria não sofrem updates de firmware automaticamente. Os fabricantes disponibilizam um portal web para configuração do equipamento com senhas por defeito, como por exemplo o tradicional admin de utilizador e admin de password.

O vídeo transmitido pode ser capturado por pessoas mal-intencionadas se não forem garantidos métodos de autenticação eficazes e uso de protocolos encriptados. Este vídeo ou as imagens capturadas, podem ser usadas para recolher informações confidenciais, perceber rotinas, explorando assim a vertente da engenharia social.

A negação de serviço, o DDoS ou a manipulação de informação são as principais falhas a que estes equipamentos estão propensos.

3.2.13. Sistema de Transporte Pneumático

Os sistemas de transporte pneumático, conhecidos como besidróglio são utilizados em unidades de saúde para enviar amostras de sangue, urina ou outras, diretamente para o laboratório de forma a evitar perca de tempo no transporte destes contentores.

São sistemas que funcionam a vácuo, onde os "torpedos" viajam numa rede de tubos espalhados por diversos locais sensíveis e que permite um transporte rápido e uma receção imediata deste tipo de cápsula.

Este sistema é controlado por um servidor que regista todos os eventos, nomeadamente que terminal envia e que terminal recebe um determinado torpedo, informando também de uma avaria caso esta ocorra, podendo especificar ao detalhe a tubagem onde ocorreu o congestionamento.

Este sistema sendo alvo de um ataque por uma pessoa mal-intencionada poderá causar negação de serviço pelo que afetará o habitual fluxo de trabalho colocando em risco o trabalho dos diversos funcionários, uma vez que a indisponibilidade deste equipamento poderá inviabilizar o envio das amostras para o laboratório, não havendo o resultado das análises atempadamente, ou poderá ter que haver necessidade de efetuar nova recolha de colheita ao utente uma vez que as amostras recolhidas podem ter sido desviadas para outro local.

3.2.14. Balanças

As balanças são usadas em unidades de saúde em diversos departamentos. Nas farmácia são utilizados para preparação de manipulados, nos laboratórios para medições de amostras clínicas, em contexto de consulta ou internamento para pesar o utente

Não é um equipamento fulcral aos cuidados de saúde nem coloca em risco a vida humana, no entanto é um equipamento que não deve ser descurado ao nível de segurança dado que possui um IP e se encontra ligado á rede, podendo uma pessoa mal-intencionada aproveitar-se das vulnerabilidades destes equipamentos para escalar privilégios na rede e conseguir acesso indevido a outros equipamentos.

3.2.15. Frigorifico

Os frigoríficos inteligentes, com ligação á rede, para monitorização constante de temperatura, encontram-se em algumas unidades de saúde, onde são guardados medicamentos que carecem de uma determinada temperatura especifica constante.

São equipamentos cuja segurança pode ser comprometida, colocando em risco outros equipamentos da rede. Pode ser utilizado como máquina de salto para chegar a outros equipamentos.

São equipamentos que em princípio não colocam em risco vidas humanas, no entanto deverão ser inventariados e identificados como potenciais portas de entrada para pessoas mal-intencionadas, uma vez que podem ser utilizados para escalar privilégios na rede em que estão ligados.

3.3. Síntese

Neste capítulo foram caracterizados os principais equipamentos ligados a uma rede numa unidade de saúde, evidenciando os principais riscos e as principais vulnerabilidades de se colocar em produção estes equipamentos sem fazer uma análise prévia ou descuidada.

Os equipamentos analisados foram segmentados em dois grupos, em equipamentos clínicos e em equipamentos de suporte ou periféricos, pelo que se evidencia em cada equipamento o papel que cada um desempenha na organização, não descurando a função que estes desempenham ressalvando para os riscos ou problemas que podem despoletar ao estarem na mesma rede.

Os equipamentos caracterizados estão suscetíveis a ficarem indisponíveis ou a comprometer os cuidados de saúde ao utente, pelo que se deverá dar especial atenção aos ataques de ramsonware, man-in-the-midle, ou de negação de serviço (DDoS). Estes ataques poderão ser nefastos para um paciente, que poderá ficar incapacitado de receber os tratamentos devidos se os equipamentos de que depende naquele instante ficarem vulneráveis ou expostos a um potencial ataque.

O capítulo que se segue apresenta as principais regras para uma implementação de equipamentos IoT em unidades de saúde, evidenciando as principais fraquezas ou fragilidades que possam advir de uma implementação que ignore estas sugestões.

4. Regras para implementação e boas práticas

Este capítulo tem como principal objetivo ajudar as equipas de profissionais que pertencem aos serviços de sistemas de informação, das demais organizações de saúde, alertar para algumas das regras de implementação, assim como evidenciar boas práticas que poderão seguir para implementar equipamentos IoT, mitigando alguns dos riscos e das vulnerabilidades elencadas no capítulo inicial.

Para que o IoT possa ser implementada de forma sustentável e segura em unidades de saúde, devem ser levadas a cabo boas práticas na sua implementação, no entanto, existem dois aspetos fulcrais. O controlo e a confiança. As equipas locais deverão ter o controlo sobre os equipamentos que instalam assim como deverão transmitir confiança aos utilizadores das unidades de saúde para o seu uso, no entanto este tipo de simbiose nem sempre se coaduna com a realidade.

Para enfrentar tais desafios, existem hoje diversos guias e frameworks que ajudam a trazer estes controlos para um projeto de IoT, nomeadamente o IoT Trust Framework [81] ou a IoT Security Guidance [82].

Estas frameworks são utilizadas por algumas organizações ao nível mundial ajudando a promover melhores práticas de segurança. Uma vez que estas frameworks não são especificamente direcionadas para unidades de saúde, foram estudados os diversos controlos de ambas e ajustados para o contexto a que este documento se propõe.

Cada modelo de negócio tem as suas particularidades diferentes, no entanto quando se trata de um bem de caracter monetário ou que envolva a nossa saúde, a motivação para comprometer a segurança ganha proporções maiores uma vez que esta afeta um bem comum a todos nós: a nossa saúde, o nosso bem-estar, o nosso futuro.

A indústria 4.0 impulsionou a inovação dos sistemas e dos negócios, apresentando uma nova dimensão e novos desafios relacionados com a gestão de novos riscos e de ciberataques.

As unidades de saúde não são exceção e o termo Hospital 4.0 [83] já está presente no nosso quotidiano. O IoT, a inteligência artificial, o big data, a impressão 3D e a realidade virtual são a nova revolução digital atual, fruto da adoção das novas tecnologias nestas instituições.

Com o propósito e com a necessidade de atender cada vez melhor o paciente e de forma a alcançar o tratamento e o bem-estar do utente, são adotadas novas estratégias de prevenção de manutenção, de gestão e de acompanhamento da saúde do utente.

Assim, a possibilidade do ser humano ficar comprometido a uma ausência de tratamentos, perante uma ameaça de morte, e por consequência se existir um suborno monetário que lhe proporcione a continuidade de tratamentos é hoje em dia uma preocupação de todos nós, quando ficamos doentes e acamados, ou dependentes de equipamentos que nos monitorizam e cuidam de nós garantido o nosso futuro.

Ao se possibilitar um atendimento único, personalizado e com um conhecimento prévio de todo o histórico de saúde de um determinado doente, a saúde ou a vida torna-se um alvo apetecível por parte de pessoas mal-intencionadas ou mais propriamente dos cibercriminosos, podendo querer lucrar com estes dados inviabilizando assim o tratamento ou a negação de cuidados a um conjunto de pessoas a uma pessoa em particular.

Os dados obtidos também podem ser usados como moeda de troca para acesso a serviços médicos de elevado custo monetário, equipamentos e prescrição de medicamentos, bem como para a aquisição fraudulenta de benefícios na área da saúde junto de seguradoras, sendo estes dados muito procurados na darkweb[4].

Os sistemas IoT partilham as características de uma rede de computadores convencional, partilhando assim os mesmo problemas de segurança que os demais equipamentos informáticos, uma vez que as transmissões na sua generalidade assentam em cima do protocolo IP.

Com a utilização destes equipamentos no nosso dia-a-dia é fundamental uma profunda reflexão e pensar como se pode proteger as informações que são recolhidas, uma vez que estes equipamentos estão cada vez mais expostos e tem sido alvo de ataques.

A ameaça constante de ataques de segurança que se tem vindo a fazer-se sentir na comunicação social e nas redes sociais, ou em fóruns desta temática, tem colocado as equipas locais dos departamentos de tecnologias de informação sobre stress e em contante alerta.

[4] Conjunto de redes encriptadas, intencionalmente escondidas da internet comum, visível apenas através de um browser específico

De salientar que as tecnologias estão cada vez mais robustas, recolhem cada vez mais informação, e os cibercriminosos procuram e anseiam constantemente este tipo de dados para poder lucrar com eles.

Diariamente são colocados scripts online para fazerem um varrimento á web mundial á procura de novos equipamentos, que possibilitem um ponto de entrada nas redes locais. Após um cibercriminoso entrar numa rede local tenta das mais variadas formas escalar privilégios para obter o acesso a equipamentos sensíveis, ou a informação confidencial. O portal shodan[84][25], por exemplo, percorre a internet e apresenta variados equipamentos expostos na internet, segmentado por tipo de equipamento e por localização.

Os dados da banca e os dados clínicos sempre foram e vão continuar a ser um tesouro muito apetecível para os cibercriminosos, dado o teor da informação aqui presente. Enquanto o acesso a dados bancários permite o enriquecimento aos cibercriminosos, por outro lado, a disponibilidade dos dados de saúde ou os dados clínicos permitem ao ser humano sobreviver, e este é um dos objetivos fundamentais da génese da nossa essência.

O ser humano anseia estar vivo, viver com qualidade, saudável e sem dificuldades, e se por alguma razão se sentir privado da saúde, ou da continuidade de tratamentos, certamente irá socorrer-se de ajuda financeira para suprimir esta necessidade.

Da análise efetuada, produziu-se a tabela 4 que poderá ser tida em consideração para implementar equipamentos IoT em unidades de saúde, validando se os equipamentos cumprem com os seguintes requisitos apresentados:

Inventariação	
	Inventariar o equipamento com um número interno
	Preenchimento da ficha de artigo/equipamento
Segurança física	
	Validar se o equipamento tem portas em funcionamento desnecessárias Ex: Usb, rj45, rs232
	Validar se o equipamento tem interfaces em funcionamento desnecessários Ex: Câmara, microfone, coluna
	Validar se o equipamento tem botão de reset facilmente acessível ou permite reposição de definições de fábrica
	Validar se o equipamento possibilita o armazenamento de dados externos
	Validar se o equipamento fica exposto ou facilmente acessível fisicamente

Acessos e privacidade	
	Validar se o equipamento valida o uso de passwords fortes
	Validar se o equipamento é suscetível a ataques XSS, SQLi ou CSRF
	Alterar a senha por defeito na primeira configuração
	Validar se após tentativas de login inválido o sistema bloqueia o utilizador
	Validar se o utilizador é notificado de acessos indevidos
	Validar se o utilizador é notificado aquando da alteração da password
	Ativar a autenticação multi-fator
	Colocar uma password única por equipamento
	Atribuir credenciais de acesso diferentes por utilizador
	Validar se a recuperação de password tem mecanismos seguros
	Validar se as passwords ficam encriptadas na base de dados
	Criar utilizadores com acessos mínimos e diferenciados
	Validar se as contas de utilizador podem ser enumeradas remotamente
	Validar se o equipamento não envia os dados para outro local (fuga de informação)
	Verificar se o equipamento recolhe apenas os dados fundamentais para a funcionalidade do equipamento
	Verificar se os dados pessoais são encriptados e protegidos
	Validar se apenas pessoas autorizadas têm acesso aos dados recolhidos do equipamento
	Validar se o equipamento é blindado e se contempla mecanismos de Reverse Engineering
Configurações insuficientes de segurança	
	Validar se o equipamento utiliza protocolos como SSL e TLS para encriptar as comunicações
	Validar se o equipamento utiliza protocolos HL7 ou DICOM
	Validar se o equipamento utiliza padrões de criptografia opensource e evita o uso de protocolos de encriptação proprietários
	Validar se o equipamento garante o registo de eventos de segurança
	Validar se o equipamento notifica os utilizadores dos eventos de segurança
Serviços de rede	
	Verificar se o equipamento é vulnerável a ataques de buffer overflow, fuzzing ou DDoS
	Verificar se o equipamento bloqueia os serviços críticos se estes forem comprometidos ou atacados
	Colocar o equipamento numa VLAN especifica
	Validar se o equipamento permite ligação por VPN ou acesso remoto
	Atribuir uma entrada especifica na firewall para o equipamento
	Analisar se o tráfego enviado é encriptado
	Verificar se existem portos abertos que não sejam necessários
	Verificar se o equipamento deteta ou bloqueia pedidos de atividade anormal
Software / Firmware	
	Verificar se o equipamento disponibiliza atualizações periódicas

	Verificar se o equipamento possibilita ligações simultâneas
	Verificar se a atualização é assinada digitalmente
	Verificar o change log das atualizações
	Subscrever alertas de atualizações no portal do fornecedor
Acompanhamento e formação	
	Validar se as equipas foram envolvidas em todos os processos (desde a compra à instalação)
	Ministrar formação aos utilizadores dos equipamentos
	Ministrar formação de cibersegurança aos restantes funcionários periodicamente
	Efetuar testes de penetração com regularidade
	Validar se existem falhas conhecidas neste tipo de equipamentos
	Efetuar uma monitorização continua, classificando as vulnerabilidades encontradas
	Subscrever alertas de vulnerabilidades para o equipamento

Tabela 3 – Check list para implementação de equipamentos IoT em Unidades de Saúde

Após análise da tabela 4, onde se apresenta um conjunto de boas práticas a ter em conta aquando da implementação de equipamentos IoT em unidades de saúde, procedeu-se á análise dos principais aspetos abordados:

4.1. Inventariação

Um dos primeiros passos na gestão da segurança das unidades de saúde começa por entender os riscos de segurança dos equipamentos interligados na rede.

Esta tarefa exige que as equipas e os profissionais dos departamentos de tecnologias de informação das organizações ou unidades de saúde, classifiquem corretamente os equipamentos sensíveis da rede, identificando quais os mais importantes de forma a priorizar esforços em caso de um ataque à segurança.

Existem variadíssimos programas para inventariação de ativos da rede, assim como programas que monitorizam constantemente a rede para encontrar novos equipamentos ativos.

À medida que a inventariação vai sendo efetuada, os equipamentos ou os equipamentos deverão ser agrupados e ordenados, pelo impacto que possam causar na rede. Os equipamentos que possuírem maior impacto ou maior risco de estarem ligados deverão ser

referenciados e deverá haver um acompanhamento mais próximo de forma a não perder o controlo sobre os mesmos.

Esta listagem de equipamentos deverá ser atualizada sempre que é adicionado um novo equipamento ou sempre que é substituído um equipamento existente. O simples facto de substituir um equipamento não garante que o firmware ou a versão de software agora presente seja a mesma que estava no equipamento antigo que foi substituído.

As listagens de equipamentos deverão ter os seguintes campos:

Nome do equipamento, número de série, modelo, IP, portos abertos, versão de software, versão de firmware, localização física, serviço a que pertence, data de instalação do equipamento, data da última verificação de atualizações, vulnerabilidades conhecidas, risco/impacto.

Existem ainda campos adicionais que podem enriquecer a listagem, nomeadamente o modelo do processador, a capacidade de memória, o protocolo de comunicação, o sistema operativo, a vlan em que foi colocado, um campo de observações, entre outros.

4.2. Segurança física

Aquando o pedido para ligação do equipamento à rede, deve ser efetuado um check-up ao equipamento ao nível físico analisando-o na integra. Esta análise visa verificar se o equipamento em questão está conforme o fabricante o enviou e deverá servir para ajudar a inventariar o equipamento, uma vez que é feito uma análise mais profunda ao hardware que apresenta.

Todas as funcionalidades que não forem necessárias deverão ser desativadas, como por exemplo a camara fotográfica, microfones, portas rs232 ou portas usb. Se por ventura existirem portas físicas que não estejam em uso, estas também deverão ser desabilitadas.

O acesso físico ao equipamento deverá ser restrito não permitindo a intrusão, como por exemplo, o reset de fábrica e o acesso com passwords por defeito. O equipamento deve ser analisado detalhadamente para se verificar se existe algum botão para efetuar este tipo de ação. Caso se verifique, poderá ser necessário proceder á blindagem do equipamento vedando o seu acesso, pelo que este tipo de ação pode ser feito com caixas próprias com cadeados, ou com a colocação de equipamentos em locais inacessíveis.

Sempre que possível, deverá ser ativada a encriptação, no entanto, aquando do processo de aquisição ou compra, deverá ser dado preferência a equipamentos que já encriptem todos os dados que transmitem.

Os equipamentos deverão ter apenas as saídas físicas estritamente necessárias, quer ao nível de portas USB, ou slots de cartões SD. Todas as portas que não são utilizadas deverão ser inutilizadas ou deverá ser vedado o acesso. Caso não seja possível bloquear o acesso ao nível de software ou de hardware, esta limitação deverá ser tratada fisicamente.

4.3. Acessos e privacidade

Estes equipamentos IoT devem possuir autenticação forte por defeito, devendo ser avaliado a implementação do uso de autenticação multi-fator (2FA) e a utilização de certificados seguros para as credenciais de acesso. Deve-se assegurar que qualquer codificação do portal web (local ou na cloud) ou no aplicativo móvel seja programado impedindo o uso de senhas fracas, incluindo mecanismos de bloqueio de conta caso existam múltiplas tentativas de acesso errado. A senha deverá expirar após um período previamente especificado se o utilizador não for efetuando um acesso pontual e deverá ser sempre solicitado a alteração do nome de utilizador e a senha aquando a primeira utilização do dispositivo IoT.

As senhas de acesso administrativo não devem ser utilizadas para outros tipos de acesso, delineando o respetivo impacto aquando do reset de fábrica. Os equipamentos devem ter acesso somente a um interface local e deverá ser registado uma senha única por dispositivo. A utilização de multi-utilizadores deve ser contemplada, elencando as funções para cada cenário e os respetivos níveis de acesso devem estar detalhados.

Os mecanismos de recuperação de senhas devem ser realizados sempre através do suporte multi-fator, seja por mensagem de texto (sms), por chamada, por gerador de códigos ou por mail desde que validado por um pin previamente definido.

As passwords locais e remotas deverão ser atualizadas para passwords fortes e de difícil memorização, sendo que cada equipamento deverá ter uma password distinta. Aconselha-se o uso de um gestor de passwords para guardar as passwords dos variados equipamentos de forma encriptada. Este gestor de passwords deverá ficar numa máquina isolada da rede, e sem ligação á internet para que não seja comprometida. A titulo de exemplo poderá ser

utilizado um telemóvel em modo de voo, com a aplicação instalada, e este equipamento deverá ser guardado em cofre próprio na instituição.

O equipamento deverá validar se a password é robusta, se tem mais do que 15 caracteres, não contem palavras conhecidas do dicionário e se é composta por números, símbolos, letras maiúsculas e letras minúsculas, aumentando assim o grau de complexidade da password. Existem gestores de password que possuem mecanismos para gerar este tipo de password, únicas e com elevado grau de complexidade.

Sempre que possível deverá ser dada preferência a compra de equipamentos IoT que possibilitem utilizar a autenticação de vários fatores, tipo autenticação 2FA.

Os acessos deverão ser atribuídos apenas quando é necessário, de forma a controlar as permissões de cada dispositivo, pelo que deverão ser criados diversos utilizadores com diversas camadas de operação.

Deverão ser descartados equipamentos que dependem de aplicações ou serviços com pouca segurança e sem privacidade.

Devem ser implementadas políticas de bloqueio, ou desativação de contas de utilizador quando são feitos ataques de brute force ou após um número razoável de tentativas de login inválidas.

Sempre que existir uma alteração de senha os utilizadores deverão ser notificados via email, e deverá ser enviado um código de validação para um dispositivo móvel para validar a alteração da senha. Estas alterações deverão ser guardadas em logs, ficando com um histórico de acessos para todos os eventos de segurança.

As credenciais de autenticação armazenadas em base de dados remotas ou nos próprios equipamentos, devem ser encriptadas, utilizando métodos de criptografia numa primeira instância com um hash, e se possível um hash com um salt para aumentar a complexidade da cifra. Os dados pessoais transmitidos também não deverão ser exceção pelo que os dados em transito deverão ser sempre encriptados.

Deve ser garantido uma credencial única de acesso por utilizador, descartando o usual *admin* para a gestão do equipamento. Cada utilizador deverá ter um login diferente, e cada login poderá ter permissões distintas, ou só de leitura, ou só escrita, ou de acesso total.

Aquando da criação do utilizador deverá ficar evidenciado quais os acessos que efetivamente necessita, pelo que os acessos deverão ser criados de forma minimalista e adicionado posteriormente mais permissões se os atribuídos inicialmente não se ajustarem com o que é expectável.

Sempre que existirem alterações de passwords ou acessos indevidos deverão ser emitidos alertas, por email ou sms para o lesado, informando por exemplo que em determinado dia e em determinado IP a password foi alterada sendo possível atuar prontamente.

Os equipamentos IoT devem possuir protocolos de segurança e criptografia atualizada e o portal web deverá ter a capacidade de utilizar o protocolo HTTPS para proteger as informações enviadas na comunicação ou partilha de informação.

O protocolo HTTPS é igual ao protocolo HTTP no entanto, esta variante utiliza certificados para proteger as comunicações entre o servidor e o cliente e vice-versa, colocando assim mais uma camada de proteção, pelo que é fulcral para evitar ataques do tipo man-in-the-middle.

A monitorização da segurança dos equipamentos deverá estar presente para reduzir possíveis impactos de vulnerabilidades e deverão ser efetuados testes a todas as vertentes web, testando as vulnerabilidades XSS, SQLi e CSRF.

A distribuição das correções de vulnerabilidades identificadas e as atualizações destas vulnerabilidades através de mecanismos eficazes não deverão modificar as configurações de utilizadores previamente configurados, nem deverão fornecer a capacidade de autorizar ou não futuras atualizações automáticas.

A recolha de dados deve ser limitada ao que for razoavelmente útil para a funcionalidade e finalidade a que se destina, pelo que devem ser avaliados os dados que realmente são necessários salvaguardando apenas os que interessam, encriptando sempre dados de cariz pessoal, ou com informações clínicas.

De forma a precaver a fuga da informação, deverá ser garantido que o equipamento não envia uma cópia dos dados para outro local, assim como deverão estar disponíveis apenas os portos estritamente necessários á atividade, devendo ser barrados outros portos na firewall de forma a mitigar este problema.

Devem também ser efetuados testes de penetração, validando se é possível enumerar os utilizadores registados, assim como as referidas passwords de cada um, tomando as medidas necessárias para evitar a exploração desta vulnerabilidade, agilizando com o fornecedor uma medida corretiva caso seja necessário.

A política de retenção de informação deverá ser de conhecimento público e disponibilizada a todos os intervenientes antes da utilização do dispositivo, pelo que deverá ser possível ao utilizador recusar qualquer política imposta sobre a partilha de informação, notificando-o dos impactos que poderá ter no funcionamento do IoT.

A anonimização de dados deverá ser garantida cumprindo com a legislação em vigor no que diz respeito ao RGPD - Regime Geral de Proteção de Dados. De salientar que deve ser garantido que apenas utilizadores autorizados tenham acesso a informações pessoais, sendo que o utilizador em questão deverá ser notificado deste acesso sempre que ocorra um evento que assim o justifique.

O equipamento deverá garantir mecanismos de blindagem que inviabilizem o reverse engineering ou a engenharia reversa, precavendo que o código seja extraído diretamente das placas de memória existente no interior do equipamento. O código ao ser extraído e ao ser analisado poderá ser fruto de uma análise mais profunda por cibercriminosos, pelo que tentarão a todo o custo encontrar pontos de entrada que poderão ser explorados futuramente.

4.4. Configurações insuficientes de segurança

As comunicações dos eventos de segurança devem ser eficientes, devendo o utilizador ser notificado por email, mensagem de texto ou outro canal de comunicação que defina sempre que estes eventos ocorram.

O idioma deverá ser padronizado por utilizador, possibilitando a seleção da linguagem com que pretende trabalhar.

Sempre que ocorram alterações ao nível de acesso o utilizador deverá ser notificado. As principais notificações a enviar centram-se aquando da alteração de password, ou em tentativas de login incorreto.

De evidenciar que todos os demais eventos de segurança deverão ficar acessíveis ao utilizador em local próprio, podendo ser consultado a qualquer instante, disponibilizando a que horas, determinado endereço despoletou uma dada ação ou qual a ocorrência efetuada.

O equipamento deverá utilizar protocolos SSL (Secure Socket Layer) e TLS (Transport Layer Security) para encriptar as comunicações. Estes protocolos proporcionam segurança na troca de dados e de informações entre aplicações, servidores e clientes que estão interligados entre si, uma vez que a troca da chave proporciona uma encriptação baseada no conteúdo do tráfego.

Os padrões de criptografia utilizados pelos equipamentos IoT deverão ser baseados em standards opensource, evitando o uso de protocolos de encriptação proprietários. A encriptação assente em standards opensource possibilita a partilha de informação ao nível mundial envolvendo a comunidade de programadores global na contribuição e numa melhoria continua deste tipo de encriptação. São tipos de encriptação que estão a ser testados constantemente pelos computadores mais potentes do mundo, criando assim um standard mais robusto e mais seguro, mais difícil de violar ou desencriptar.

De forma a garantir padrões mundiais de interoperabilidade, os equipamentos IoT que operam com dados clínicos, deverão transmitir os dados com normas de comunicação conhecidas nomeadamente o HL7 ou o DICOM. Estes tipos de normas de comunicação são standards utilizados ao nível global onde é garantida a disponibilização da informação com a integridade desejada. Estes padrões estão dotados de um conjunto de regras que permitem que a informação seja partilhada e interpretada de forma consistente, permitindo que diferentes aparelhos comuniquem entre si com a mesma linguagem.

4.5. Serviços de Rede

Com uma correta segmentação da rede, categorizando os equipamentos por níveis, dados e em grupos específicos, é possível restringir o acesso e a comunicação entre as diversas camadas. A criação destes limites permite restringir o tráfego, controlando o fluxo de informação, identificando facilmente os fluxos de comunicação suspeitos.

A segmentação da rede previne também o roubo de informações e a propagação de malware, pelo que dá confiança ás equipas locais dos sistemas de informação para adoção de novas soluções de equipamentos IoT, ao mesmo tempo que oferecem uma nova camada de segurança e proteção de dados, sem comprometer a sua performance e fiabilidade.

Assim com a segmentação da rede é possível evitar o roubo de dados clínicos ou que a criptografia de malware se propague pela rede, isolando a ameaça em determinado nível.

A separação dos dados clínicos da restante rede oferece aos profissionais das equipas de tecnologias de informação uma visão mais clara do tráfego da rede para detetar situações anómalas que poderão indicar um equipamento comprometido.

Como verificado no capítulo anterior, na mesma rede pode existir por exemplo uma impressora a operar na mesma vlan que um monitor de sinais vitais, pelo que este tipo de abordagem deverá ser muito bem equacionada, limitando o mais possível de forma a que dados sensíveis não naveguem na mesma rede que dados vulgares.

Esta segmentação é possível com a criação de vlans, restringindo sempre o acesso á internet ou ao exterior ao estritamente necessário, pelo que se deverá avaliar bem o impacto destes equipamentos de rede, aquando da sua colocação em produção.

Os diversos dispositivos ou equipamentos IoT deverão ser colocados numa rede separada, com firewall e com monitorização de tráfego, pelo que deverá ser dado preferência a equipamentos que possibilitem o uso de VPN para a sua gestão e para a monitorização dos mesmos. Este tipo de equipamento não deverá permitir ligações automáticas à rede Wi-Fi sob forma de ser iludido por routers com o mesmo SSID pelo que poderia ficar a enviar dados para o gateway errado.

Ao aceder-se a um equipamento por VPN estamos a incrementar mais uma camada de segurança, uma vez que a comunicação é efetuada por um túnel virtual, onde são aplicados mecanismos de proteção, que impedem conhecer o trafego que circula, bem como o destinatário ou o remetente.

Toda a exceção que seja criada, deverá ser claramente identificada na tabela de inventário previamente criada, de forma a mitigar o risco que este equipamento possa impactar na rede, evitando ao máximo a exposição para o exterior de equipamentos que poderão ter vulnerabilidades já conhecidas.

De realçar que deverá ser considerado o uso de firewalls de perímetro para proteger todas as interfaces da rede, permitindo apenas o estritamente necessário ao desempenho das funções.

O futuro do IoT foca-se em tornar uma rede de equipamentos autónomos que podem interagir uns com os outros e tomar decisões inteligentes sem intervenção humana. É nesta

fase que o blockchain pode ajudar esta tecnologia a dar o salto e a formar uma base sólida que suportará a transação das comunicações de forma mais segura e única.

O blockchain pode ser usado para preservar e proteger dados no âmbito do IoT uma vez que poderá ser possível analisar todas as transações efetuadas.

A encriptação é um dos eixos fundamentais para que esta tecnologia vingue e ganhe a credibilidade que tem sido abalada ultimamente. Ao proceder-se à encriptação dos dados, passará a ser mais difícil analisar o teor das comunicações, garantido uma confidencialidade nas transações efetuadas.

O desempenho dos equipamentos deverá ser monitorizado constantemente para validar se está a efetuar apenas a função que lhes compete, verificando se não existe consumo de tráfego anormal ou se a informação está a ter o destino esperado.

Todo o tráfego gerado pelos equipamentos IoT deverá ser analisado, com programas tipo o Wireshark, ou Tcpdump para perceber se o equipamento está a encriptar as comunicações e se está a recolher ou a enviar o estritamente necessário.

Deverá também ser analisado o tráfego que o equipamento recebe e transmite e verificar se existem portas no software abertas que podem permitir o controle remoto.

Poderá ser efetuado uma bateria de testes de forma a precaver os ataques de buffer overflow, de fuzzing ou de negação de serviço. Estes ataques tem como principal objetivo tornar o equipamento indisponível, pelo que o equipamento deverá saber interpretar que está a ser alvo de um ataque e deverá bloquear serviços críticos se estes forem comprometidos, enviando alarmística para a equipa local de sistemas de informação de forma a esta agir em conformidade o mais rapidamente.

4.6. Software e firmware

Um equipamento IoT atualizado, quer ao nível de software, quer ao nível de firmware, é fundamental para que possíveis invasores não explorem falhas já conhecidas. Assim deve haver um controlo das versões instaladas em cada equipamento devidamente documentadas na ficha de equipamento.

O controlo de versões deverá ser registado, ativado, e deverão ser efetuadas subscrições de alertas com os fornecedores, de forma a que estes enviem automaticamente um email sempre que exista um novo update informando assim as equipas locais de sistemas de informação.

Deverá existir uma monitorização ativa e um fluxo interno bem delineado para verificar se existem novas atualizações e novos updates, de forma a prevenir problemas de segurança da rede.

Antes de se efetuar uma atualização deverá ser estudado atentamente o change log. Este ficheiro é fornecido pelo fabricante, com todas as alterações efetuadas desde a ultima atualização, de forma a validar se as atualizações a efetuar se coadunam com o que é pretendido, e se não vai prejudicar o seu propósito de atuação.

O firmware e o software deverão estar sempre atualizados com as mais recentes atualizações, uma vez que o fabricante sempre que deteta uma vulnerabilidade corrige o problema e disponibiliza o respetivo firmware. As atualizações automáticas deverão ser ativadas, no entanto e de forma a possibilitar uma melhor gestão, deverão ser subscritos alertas junto dos fabricantes a notificar a necessidade de atualização de equipamentos. Este documento deverá ser lido com atenção, uma vez que o fabricante ao fazer uma determinada atualização poderá estar a comprometer a segurança, ao alterar algo que não seria expectável.

As atualizações deverão ser assinadas digitalmente de forma a não comprometer a segurança da rede com um update de firmware que não seja do fabricante, ou que já possa ter sido alterado ou manipulado por outro.

Os equipamentos que não recebem atualizações deverão ser identificados e deverão ser retirados de funcionamento ou isolados na rede. Estes equipamentos são alvos apetecíveis por parte dos cibercriminosos que tentam encontrar uma vulnerabilidade que permitirá o acesso á rede, sabendo de antemão que este acesso estará sempre ativo, dado o equipamento não sofrer mais atualizações.

A subscrição de alertas no portal do fornecedor também deverá ser ativada, para receber alertas automáticos para determinado equipamento caso seja encontrada uma vulnerabilidade, ou se for disponibilizada uma nova atualização para download.

O equipamento deverá possibilitar ligações simultâneas sem causar qualquer constrangimento no regular funcionamento do mesmo. Deverá ser garantido que os dados

enviados e recebidos chegam ao destinatário correto, independentemente de existirem outros clientes ligados ao equipamento.

Os fabricantes deveriam ter como dado obrigatório a adoção do SSDLC (Secure Software Development Lifecycle) [85], que incorpora modelos de ameaças de forma a prevenir estes ataques.

4.7. Acompanhamento e formação

O acompanhamento e o envolvimento das equipas de informática é fulcral em todas as fases. Estas equipas deverão ser integradas num primeira instância para efetuar o levantamento das necessidades de cada equipamento, sugerindo o melhor artigo a comprar, considerando sempre a segurança como ponto fundamental.

Na fase da implementação deverão ser envolvidas também as equipas no terreno, colocando o equipamento em produção, procedendo aos testes necessários, e á respetiva inventariação.

A cibersegurança está em constante evolução, pelo que as equipas de tecnologias necessitam de estar permanentemente atualizadas sobre as ameaças mais recentes. Ao dotar estes profissionais e estas equipas de formação especifica será possível criar melhores defesas e também uma maior consciencialização para os restantes funcionários sobre os ataques e fraudes que poderão acontecer.

A cibersegurança exige um trabalho diário de equipa com todos os membros da organização envolvidos na identificação de possíveis vulnerabilidades ou ameaças, alertando os demais funcionários envolvidos para não serem vítimas de qualquer tipo de ataque, consciencializando os profissionais para os ataques de engenharia social. Os ataques de engenharia social tem vindo a ganhar adeptos, pelo que um cibercriminoso ao conseguir obter informação adicional de um determinado funcionário, pode ajustar o seu espectro de ação com base na informação recolhida.

De forma a criar uma rede segura, e um ecossistema interno isento de riscos, as equipas de tecnologias de informação das mais variadas unidades de saúde, devem saber lidar com as vulnerabilidades que vão encontrando nos equipamentos que vão instalando e deverão ser equipas pró-ativas, jogar sempre na defensiva, pelo que deverão estar em constante formação.

A formação deverá ser essencialmente em proteção e em medidas de defesa, dado que neste tipo de área é muito difícil prever os problemas que poderão advir. Todos os dias existem novas formas, novas táticas, novas técnicas e novos modos de operação.

A forma como se reage ou atua depois de um ciberataque também deverá ser equacionado, e os profissionais deverão estar consciencializados para essa realidade.

A formação deverá incidir sobre ataques conhecidos, que já tenham ocorrido em outras instituições e assim aprender com os erros cometidos por outras equipas melhorando o know-how interno.

Os profissionais que utilizem a rede interna deverão ser sensibilizados para este tipo de risco, pelo que periodicamente poderão ser feitos pequenos testes, como por exemplo o envio de emails falsos tipo pishing, de forma a identificar as fraquezas internas e a poder direcionar a formação a um grupo de funcionários restritos onde a sua cultura de defesa ou de cibersegurança seja mais urgente. É comum os funcionários internos caírem em esquemas de engenharia social, nomeadamente provenientes de emails, que por sua vez despoletam a instalação de software malicioso colocando em risco a restante rede.

Alguns equipamentos IoT na sua génese necessitam de software extra para se poderem configurar, pelo que deverá existir uma cultura de defesa e um nível de desconfiança que faça sempre duvidar qualquer tipo de ação anómala.

Deverá ser ministrada formação aos utilizadores da rede, uma vez que cada vez mais ocorrem ataques de engenharia social, sendo os próprios funcionários os intervenientes nos ataques, assim é fulcral educar os utilizadores dos equipamentos sobre os riscos de segurança e os problemas que advém da utilização de equipamentos IoT.

É fundamental que as equipas locais fomentem uma cultura severa e rígida ao nível de segurança, alegando que os equipamentos IoT são provavelmente mais vulneráveis do que os dispositivos tradicionais apresentando evidencias, provas e factos.

O amplo leque de funcionários deve ser sensibilizado para que inadvertidamente possam facilmente cair num ataque de pishing ou num ataque de engenharia social. Esta sensibilização pode ser feita com formação, e campanhas internas de divulgação de boas práticas.

Aquando da sua implementação, é fundamental que se efetuem testes funcionais para validar a integridade e o desempenho do dispositivo.

Os testes de penetração (pentest) são muito uteis para dar ás equipas locais de tecnologias de informação quais as vulnerabilidades que um dado equipamento detém, assim como perceber onde atuar para mitigar problemas que possam causar muito impacto.

Os testes de penetração exploram as fraquezas já conhecidas, existentes em determinados equipamentos. Estes testes também permitem identificar se os demais equipamentos podem levar a violação de informação sensível ou a atividades maliciosas.

Após um teste deve ser sempre gerado um relatório onde fica um resumo das vulnerabilidades encontradas e as respetivas formas de mitigação.

Deverão ser feitos testes de penetração com regularidade para encontrar novas vulnerabilidades nos equipamentos, no entanto é de salientar os limites impostos pela lei do cibercrime, lei nº 109/2009 de 15 de setembro.

Com as vulnerabilidades encontradas, deverá ser classificado o equipamento com o respetivo risco que poderá trazer á instituição, pelo que estes dados deverão ficar de fácil consulta na ficha do equipamento.

A capacidade de testar um ataque e verificar como estão as equipas preparadas para uma ciberdefesa também é um ponto chave que deverá ser trabalhado. Este tipo de testes ajuda a melhorar o tempo de resposta a ataques e aumenta a eficiência na defesa, uma vez que existe uma maior consciencialização para os riscos e perigos a que estão sujeitos.

Apesar das demais medidas preventivas implementadas pelas organizações, estas ainda enfrentam variadíssimas falhas de segurança. Assim é fundamental a implementação de algoritmos de deteção de intrusões (IDS) e sistemas de prevenção contra invasões (IPS), software antivírus, firewall e um sistema de gestão e correlação de eventos de segurança (SIEM) para ajudar a detetar falhas de segurança no seu período inicial.

A deteção de falhas pode ser efetuada com testes de penetração, com pesquisa em páginas da atualidade e com o acompanhamento dos mais recentes CVE (Common Vulnerabilities and Exposures). Estas páginas são públicas e é possível subscrever alertas para receber email sempre que exista uma vulnerabilidade nova.

Também existem sites governamentais que podem ser consultados, como é o caso do Centro Nacional de Cibersegurança (CNC) que possuem informações atualizadas das ameaças mais comuns.

Depois de colocar em produção novos equipamentos é fundamental verificar se estes equipamentos colidem com outros e se colocam em risco algum outro equipamento.

É fundamental que se efetue uma monitorização continua de forma a encontrar novas vulnerabilidades nos equipamentos.

As vulnerabilidades encontradas deverão ser designadas ao equipamento onde foram encontradas, na folha de inventário, onde facilmente se poderá consultar todo o histórico do equipamento centralizando assim a informação num único local.

Deverá também ser usada uma escala de 0 a 10 para identificar o risco, sendo o risco baixo, médio, alto ou crítico em função do impacto que causa.

A vulnerabilidade deverá ser descrita, com um resumo do tipo de ataque possível e o seu possível impacto, devendo esta informação ficar centralizada, na ficha do equipamento aquando da sua inventariação.

4.8. Síntese

No decorrer deste capítulo foi elaborada uma tabela que poderá servir de guião para implementar os equipamentos IoT em unidades de saúde. Esta tabela poderá ser utilizada como checklist com vários tópicos que poderão ser analisados e validados.

Este capítulo apresenta na sua génese um conjunto de regras de boas práticas para a implementação de equipamentos IoT de forma a proteger os dados críticos e sensíveis da organização.

Como tópicos fundamentais, ao longo deste capítulo é abordada a necessidade de uma correta inventariação, elencando os campos que deverão ser preenchidos de forma a identificar inequivocamente cada equipamento. É também abordada a segurança física evidenciando a necessidade de proteger e desabilitar as portas ou os periféricos que não são utilizados.

Os acessos e a privacidade dos dados pessoais também são abordados dando especial atenção á alteração das passwords por defeito e aos alertas de segurança que deverão ocorrer sempre que existam eventos de segurança que assim o exijam..

Segue-se uma abordagem ás configurações insuficientes de segurança, aos serviços de rede e á necessidade da criptografia nas comunicações-

A importância das atualizações dos equipamentos também tem o seu destaque, sendo este tema precedido do acompanhamento e da necessidade de ministrar formação aos demais funcionários, de forma a estes se consciencializarem da importância dos equipamentos.

Com as boas práticas apresentadas neste capítulo, pretende-se dotar as unidades de saúde de e as equipas de suporte dos sistemas de informação de um mecanismo que servirá de guião para ajudar na implementação de IoT de forma mais concisa respeitando um conjunto de passos que até ao momento era feito de forma ineficiente.

O desenho desta checklist visa colmatar os problemas identificados no capítulo 3, onde são abordados problemas com os variadíssimos equipamentos IoT presentes numa unidade de saúde, sabendo de antemão, após leitura do capítulo 2, os principais ataques, os riscos e as vulnerabilidades a que estão propensos .

Para concluir esta dissertação, elaborou-se o capítulo que se segue onde foram consolidados os temas aqui abordados.

5. Conclusão

O setor da saúde tem enfrentado inúmeros desafios, atendendo que deixou de utilizar o papel, para efetuar o registo em formato digital com derivado da evolução tecnológica. Estes sistemas, na sua génese não foram projetados em torno da segurança digital. Com o aumento do valor das informações clínicas, as unidades de saúde necessitam de encontrar maneiras de avaliar corretamente os fornecedores e os equipamentos antes de instalá-los.

À medida que o número de equipamentos ligados à rede aumenta, as equipas de tecnologias de informação necessitam de determinar como lidar com os dados e com a segurança destes equipamentos. Para que os equipamentos IoT em unidades de saúde sejam realmente transformadores e tenham a utilidade pretendida, as organizações de saúde necessitam de descobrir como transformar todos os dados recolhidos. Embora esta transformação esteja em profundas alterações, será necessário que os administradores, os fabricantes e os fornecedores de equipamentos IoT para unidades de saúde trabalhem juntos para impulsionar o desenvolvimento e garantir a segurança dos dados que são partilhados entre os demais equipamentos garantindo a confidencialidade e a integridade da informação.

Os benefícios que os equipamentos IoT em unidades de saúde oferecem são variadíssimos e não podem ser ignorados, uma vez que oferecem ou possibilitam aos utentes, aos prestadores de serviços de saúde e aos demais profissionais da instituição informações potencialmente vitais para ajudar na cura ou no fluxo dos processos de trabalho do dia-a-dia. No entanto estas unidades de saúde devem estar cientes dos riscos e das vulnerabilidades que acompanham estes equipamentos, garantindo sempre a melhor prestação de cuidados de saúde ao utente, sem nunca comprometer o desempenho ou a confiabilidade do tratamento a adotar.

Os principais objetivos desta dissertação focam-se em identificar e caracterizar os equipamentos IoT presentes em unidades de saúde, assim como na identificação os riscos e vulnerabilidades a que estão sujeitos.

Foi abordado o estado da arte onde se evidenciou os tipos de comunicação e a sua evolução, face ás necessidades destes equipamentos. Os protocolos de comunicação dos equipamentos IoT que têm acompanhado a evolução das comunicações e as principais normas de comunicação também foram abordadas de forma a perceber quais os standards em vigor.

A motivação para comprometer a segurança também foi um tema abordado neste capítulo, assim como os principais ataques de segurança e os tipos de ameaça a que cada equipamento está propensos.

Os demais equipamentos IoT que se podem encontrar em unidades de saúde foram caracterizados, apresentando alguns riscos e vulnerabilidades a que cada equipamento está suscetível.

Foram abordados os principais equipamentos IoT que se encontra em unidades de saúde, fazendo referência aos principais problemas e ataques que estes podem potenciar no desempenhar das sua funções.

São equipamentos na sua génese que monitorizam dados sensíveis, com parâmetros vitais importantes para um melhor diagnostico e tratamento do doente, e outros equipamentos mais vulgares no nosso quotidiano, como por exemplo uma smartTV ou uma impressora, que não lidam diretamente com dados fulcrais, mas são equipamentos que podem potenciar um possível ataque.

Os cibercriminosos podem desencadear ações para identificar os equipamentos que são mais vulneráveis a um ataque, e assim escalar privilégios de domínio da rede, de forma a obter um controlo diferenciado e eficaz.

Este equipamentos mais vulgares e que são utilizados no dia-a-dia podem facilmente cair em esquecimento ao nível de suporte pelas equipas locais dos sistemas de informação. A ausência de atualizações de firmware é um dos principais pontos de exploração de vulnerabilidades por parte dos cibercriminosos.

No desenrolar desta dissertação, procedeu-se á criação de uma check-list com regras de boas práticas para instalar equipamentos IoT em unidades de saúde. Este capítulo assenta numa tabela que poderá ser utilizada como orientação para instalar equipamentos IoT em unidades de saúde.

As arquiteturas IoT existentes, atualmente preocupam-se mais com os problemas de funcionalidade e usabilidade do que na problemática da segurança do sistema em si, principalmente ao nível dos dados.

A segurança é um elo inimigo da funcionalidade e do desempenho, uma vez que sobrecarregam os equipamentos, esgotam recursos e isso traduz-se numa experiência e numa usabilidade negativa para o utilizador final.

De salientar que, por muitas medidas preventivas que se tomem, diariamente existem novas descobertas, novos vetores de ataques, cada vez mais hackers curiosos, pelo que é impossível cobrir todos os ataques e vulnerabilidades possíveis. No entanto deve-se trabalhar na antecipação aplicando as regras apresentadas. O problema da segurança nos IoT em unidades de saúde é uma questão muito sensível pelo que não pode ser descurada.~

As regras de implementação de equipamentos IoT apresentadas neste trabalho podem ser utilizadas por qualquer unidade de saúde em território nacional ou internacional. São guidelines que podem ser implementadas em qualquer organização que disponibilize dados de saúde e de teor confidencial, como por exemplo centros de saúde, hospitais, clínicas, laboratórios ou farmácias.

Estas unidades de saúde, ao seguirem este conjunto de boas práticas, vão ficar elucidadas dos riscos que um simples equipamento pode ter ao ser colocado na rede. Por mais inofensivo que um equipamento possa parecer, deverá haver sempre uma cultura de segurança e monitorização constante.

Sabendo que os equipamentos IoT foram desenhados a pensar na funcionalidade e na simplicidade acima de tudo, torna-se difícil conseguir encontrar uma arquitetura que permita adicionar segurança ao nível dos dados e da privacidade do utilizador, no entanto deverão ser tidas em conta as considerações elencadas no capítulo anterior.

Os equipamentos IoT em unidades de saúde têm que funcionar obrigatoriamente em conjunto com padrões de interoperabilidade de forma a criar uma camada que encapsule a informação e a transmita para o destinatário de forma encriptada e segura, com os dados padronizados.

Como medidas preventivas é perentório que se proceda a uma atualização do software e dos firmwares, contemplando as últimas releases de segurança de cada equipamento, rever as políticas de segurança, desativar as portas dos equipamentos que não são utilizadas, e consciencializar os utilizadores dos riscos que estes equipamentos estão propensos, criando uma cultura de segurança, e evidenciando o uso de passwords fortes e encriptadas.

Qualquer que seja o vetor por onde se aborde este problema de segurança, está presente que ainda existe muito trabalho pela frente no que toca à definição e adoção de padrões. Seja do lado dos fabricantes seja do lado do consumidor final.

O problema das ameaças internas nas organizações é um dos temas mais complicados ao nível da segurança de informação. Pode-se minimizar o risco ao instalar os últimos updates de firmware, ao investir no rigor da credenciação dos funcionários, bem como na formação dos colaboradores internos, mantendo-os a par das ameaças e das práticas correntes para ludibriar os sistemas assim como efetuando uma vigilância apertada com especial atenção à alteração comportamental. No entanto o fator chave da segurança contra a ameaça interna é sem qualquer dúvida o fator humano e a sua consciencialização para este problema.

Para um completo aproveitamento de todo o potencial dos equipamentos IoT ainda existe um longo caminho a traçar, no entanto a consciencialização para os problemas de segurança têm vindo a ganhar cada vez mais adeptos.

Posso afirmar que é praticamente impossível ter um sistema completamente isento de riscos e de vulnerabilidades, no entanto as boas práticas se forem aplicadas ajudam a minimizar o impacto e a tornar os sistemas mais robustos e imunes a ataques, uma vez que quanto maior o valor do teor da informação que é transmitida pelos equipamentos IoT, mais adeptos e cibercriminiosos estarão a tentar obter e alcançar estes dados para poder lucrar com ela.

5.1. Trabalho futuro

Como trabalho futuro pretende-se alargar estas regras de boas práticas a outros equipamentos de saúde que não tenham sido abordados no âmbito deste documento ou que entretanto tenham surgido no mercado.

Depois de um equipamento ser atacado o teor de informação que permanece nele é reduzido pelo que outro ponto de partida como trabalho futuro seria estudar qual a possibilidade de se efetuar uma análise forense a um equipamento IoT comprometido.

Outro aspeto importante a considerar futuramente será o uso do blockchain na partilha de informações e na salvaguarda de dados clínicos de cada paciente.

De salientar que também é muito importante definir um plano bem estruturado de resposta a incidentes, de forma a dar continuidade ao negócio em caso de um ataque ou de indisponibilidade dos sistemas.

Por último, sugere-se a criação de uma plataforma web para gestão de equipamentos IoT totalmente vocacionado para esta realidade, com índices de risco e analise de vulnerabilidades automáticas, que poderá ser utilizado em qualquer cenário de negócio 4.0.

Referências Bibliográficas

[1] R. I. Hdowkfduh *et al.*, "Survey of Smart Healthcare Systems using IOT," vol. 6, pp. 508–513, 2018.

[2] A. Carolina, B. Monteiro1, R. Padilha, and V. V Estrela, "Health 4.0: Applications, Management, Technologies and Review Type of article: Review," *Med. Technol. J.*, vol. 2, no. 2, pp. 262–276, 2019.

[3] K. L. Lueth, "State of the IoT 2018: Number of IoT devices now at 7B - Market accelerating," *IoT Analytics*, 2018. [Online]. Available: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/.

[4] M. Hung and V. President, "Gartner Insights on How to Lead in a Connected World," 2017.

[5] "Número total de dispositivos ligados à internet." [Online]. Available: https://iot-analytics.com/wp/wp-content/uploads/20.

[6] S. Semester, *Proceedings of the Seminar Sensor Nodes – Operation, Network and Application (SN)*. 2012.

[7] P. Scully, "The Top 10 IoT Segments in 2018 – based on 1,600 real IoT projects." [Online]. Available: https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/.

[8] K. Plathong and B. Surakratanasakul, "A study of integration Internet of Things with health level 7 protocol for real-time healthcare monitoring by using cloud computing," *BMEiCON 2017 - 10th Biomed. Eng. Int. Conf.*, vol. 2017-Janua, pp. 1–5, 2017.

[9] Vodafone, "Vodafone claims internet of things connected healthcare can improve millions of lives and save billions of dollars," 2017. [Online]. Available: https://www.vodafone.com/business/news-and-insights/press-release/vodafone-claims-internet-of-things-connected-healthcare.

[10] J. Rice, "Monitoring Parkinson's disease with sensors and analytics to improve

clinical trials," 2017. [Online]. Available: https://www.ibm.com/blogs/research/2017/04/monitoring-parkinsons-disease/.

[11] M. V. Studio, "Gojo," 2015. [Online]. Available: https://www.youtube.com/watch?v=_pQNoLKrSoA.

[12] C. Swedberg, "IntelligentM Wristband Monitors Hand Hygiene, Vibrates to Provide Staff Alerts," 2013. [Online]. Available: http://www.rfidjournal.com/articles/view?10558.

[13] T. Guardian, "Google tests smart contact lens for diabetics," 2014. [Online]. Available: https://www.theguardian.com/technology/2014/jan/17/google-tests-smart-contact-lens-diabetics.

[14] M. L. Chun-lei, "Roche," 2017. [Online]. Available: https://customers.microsoft.com/en-us/story/roche-diagnostics.

[15] F. and D. Administration, "FDA approves first automated insulin delivery device for type 1 diabetes," 2016.

[16] C. and E. Barb Edson - General Manager, Marketing, "Weka," 2016. [Online]. Available: https://blogs.microsoft.com/iot/2016/08/16/iot-enabled-smart-fridge-helps-manage-vaccines-and-saves-lives/.

[17] R. Ortega, "Btt Corp," 2017. [Online]. Available: https://customers.microsoft.com/en-us/story/btt.

[18] V. Yang, "Zion China," 2017. [Online]. Available: https://customers.microsoft.com/en-us/story/zionchina.

[19] K. J. G. Schmailzl, "Hospital Ruppiner Kliniken," 2017.

[20] A. j G. & Co, "Medical Device Cybersecurity, regulatory Oversight & Insurance," no. September, 2017.

[21] Swati Khandelwal, "Medtronic's Implantable Defibrillators Vulnerable to Life-Threatening Hacks," 2019. [Online]. Available: https://thehackernews.com/2019/03/hacking-implantable-defibrillators.html.

[22] Santa Casa da Misericórdia do Porto, "Hospital da Prelada será o primeiro 'Smart

Hospital' em Portugal," 2018. [Online]. Available: http://www.w11stop.com/blogs/wp-content/uploads/2017/09/How-IoT-will-benefit-Healthcare-1.jpg.

[23] CISA, "Medtronic MiniMed 508 and Paradigm Series Insulin Pumps," 2019. [Online]. Available: https://www.us-cert.gov/ics/advisories/icsma-19-178-01.

[24] A. Medtronic, "Circular Informativa N. º128/CD/550.20.001," pp. 2–5, 2019.

[25] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing medical device vulnerabilities on the Internet of Things," *2017 IEEE Int. Conf. Intell. Secur. Informatics Secur. Big Data, ISI 2017*, pp. 176–178, 2017.

[26] "Diagrama de conectividade." [Online]. Available: https://www.postscapes.com/wp-content/uploads/2018.

[27] "Protocolos de rede IoT e sua aplicação." [Online]. Available: https://www.embarcados.com.br/wp-content/uploads/2.

[28] H. Zhang, J. Li, B. Wen, Y. Xun, and J. Liu, "Connecting intelligent things in smart hospitals using NB-IoT," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1550–1560, 2018.

[29] H. Choi, N. Kim, and H. Cha, "6LoWPAN-SNMP: Simple network management protocol for 6LoWPAN," *2009 11th IEEE Int. Conf. High Perform. Comput. Commun. HPCC 2009*, pp. 305–313, 2009.

[30] J. Hui and A. R. Corporation, "RFC 6282: Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," pp. 1–24, 2011.

[31] T. Winter, P. Thubert, A. R. Corporation, and R. Kelsey, "RFC 6550: IPv6 Routing Protocol for Low-Power and Lossy Networks," pp. 1–157, 2012.

[32] S. C. Ergen, "ZigBee/IEEE 802.15. 4 Summary," *UC Berkeley, Sept.*, vol. 10, p. 17, 2004.

[33] J. Decuir, "Bluetooth Smart Support for 6LoBTLE: Applications and connection questions," *IEEE Consum. Electron. Mag.*, vol. 4, no. 2, pp. 67–70, 2015.

[34] T. Y. Wu and W. T. Lee, "The research and analysis for rear view transmission based on ieee 802.11 wireless network," *Proc. - 2014 10th Int. Conf. Intell. Inf. Hiding*

Multimed. Signal Process. IIH-MSP 2014, no. Ieee 802, pp. 646–649, 2014.

[35] S. S. Park, "An IoT application service using mobile RFID technology," *Int. Conf. Electron. Inf. Commun. ICEIC 2018*, vol. 2018-Janua, pp. 1–4, 2018.

[36] ECMA International, "Near Field Communication - Interface and Protocol (NFCIP-1)," no. June, p. 52, 2013.

[37] W. Rzepecki, L. Iwanecki, and P. Ryba, "IEEE 802.15.4 thread mesh network - Data transmission in harsh environment," *Proc. - 2018 IEEE 6th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2018*, pp. 42–47, 2018.

[38] M. T. Buyukakkaslar, M. A. Erturk, M. A. Aydin, and L. Vollero, "LoRaWAN as an e-Health Communication Technology," *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 2, pp. 310–313, 2017.

[39] J. R. E. Leite and P. S. Martins, "A Internet das Coisas (IoT) : Tecnologias e Aplicações," no. December, 2017.

[40] D. Soni and A. Makwana, "A survey on mqtt: a protocol of internet of things(IoT)," *Int. Conf. Telecommun. Power Anal. Comput. Tech. (Ictpact - 2017)*, no. April, pp. 0–5, 2017.

[41] M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, and R. Al-Hatmi, "Internet of Things: Survey and open issues of MQTT protocol," *Proc. - 2017 Int. Conf. Eng. MIS, ICEMIS 2017*, vol. 2018-Janua, pp. 1–6, 2018.

[42] K. H. e C. B. Zach Shelby, "RFC 7252: The Constrained Application Protocol (CoAP)," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.

[43] H. A. Khattak, M. Ruta, E. Eugenio, and D. Sciascio, "CoAP-based healthcare sensor networks: A survey," *Proc. 2014 11th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2014*, pp. 499–503, 2014.

[44] R. T. Fielding *et al.*, "RFC 2616: Hypertext Transfer Protocol," pp. 1–114, 1999.

[45] S. P. Jaikar and K. R. Iyer, "A Survey of Messaging Protocols for IoT Systems," *Int. J. Adv. Manag. Technol. Eng. Sci.*, vol. 8, no. II, pp. 510–514, 2018.

[46] "HL7 international," 2019. [Online]. Available:

https://www.hl7.org/implement/standards/index.cfm?

[47] A. da Republica, "Diário da República, 1.ª série — N.º 143 — 26 de julho de 2017," pp. 5688–5724, 2017.

[48] L. Janeiro, N. Matela, N. Oliveira, and P. Almeida, "Imagem Digital em formato DICOM : Conteúdo e Estrutura Digital Imaging in DICOM format : Its Content and Structure," pp. 73–79, 2011.

[49] O. Foundation, "Open industry specifications, models and software for e-health," 2011. .

[50] Eleanor Dickinson, "Melbourne heart clinic hit by ransomware attack," *ARN*, 2019. [Online]. Available: https://www.arnnet.com.au/article/658014/melbourne-heart-clinic-hit-by-ransomware-attack/.

[51] I. T. e R. Au-Yong, "SingHealth cyber attack: How it unfolded," *Straitstimes*, 2018. [Online]. Available: https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

[52] B. J. Sanborn, "UnityPoint Health System hit with cyberattack affecting 16,000 patients," *Healthcare Finance News*, 2018. [Online]. Available: https://www.healthcarefinancenews.com/news/unitypoint-health-system-hit-cyberattack-affecting-16000-patients.

[53] M. Field, "WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled," *Technology Intelligence*, 2008. [Online]. Available: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

[54] S. Ragupathy and M. Thirugnanam, "IoT in Healthcare : Breaching Security Issues Security Breaches and Threat Prevention in the Internet of Things," *Adv. Inf. Secur. Privacy, Ethics (AISPE), B. Ser.*, no. February, 2017.

[55] R. Maria and O. Ribeiro, "Segurança em IoT: simulação de ataque em uma rede RPL utilizando Contiki," p. 70, 2018.

[56] L. S. Medeiros, P. E. Strauss, D. Sc, M. Sc, and M. Sc, "Segurança da informação

para desenvolvimento e utilização de IoT," 2017.

[57] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of Security and Privacy Issues of IoT," pp. 1–7, 2012.

[58] ENISA, *Good Practices for Security of Internet of Things in the context of Smart Manufacturing NOVEMBER 2018 Good practices for Security of Internet of Things in the context of Smart Manufacturing About ENISA*, no. November. 2018.

[59] ENISA, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*, no. November. 2017.

[60] S. Krushang and H. Upadhyay, "A survey on Internet of Things," *Int. J. Eng. Res. Dev.*, vol. 10, no. 11, pp. 58–63, 2014.

[61] Garcia-Morchon, "RFC 8576: Internet of Things (IoT) Security: State of the Art and Challenges," pp. 1–50, 2019.

[62] M. Digital, "Segurança em Redes de Computadores," pp. 1–8, 2013.

[63] S. Patients, D. Against, G. Threats, and B. Cybersecurity, "Securing the Internet of Healthcare Things The current threat landscape for the EoT The challenge for organizations," pp. 1–12, 2018.

[64] H. Journal, "89 Percent of Healthcare Organizations Have Experienced a Data Breach," *HIPAA Journal*, 2016. [Online]. Available: https://www.hipaajournal.com/ponemon-89-pc-healthcare-organizations-experienced-data-breach-3430/.

[65] H. Journal, "87% of Healthcare Organizations Will Adopt Internet of Things Technology by 2019," *HIPAA Journal*, 2017. [Online]. Available: https://www.hipaajournal.com/87pc-healthcare-organizations-adopt-internet-of-things-technology-2019-8712/.

[66] R. C. Keith A. Stouffer, "Measuring Impact of Cybersecurity on the Performance of Industrial Control Systems," *NIST*, 2014. [Online]. Available: https://www.nist.gov/publications/measuring-impact-cybersecurity-performance-industrial-control-systems.

[67] M. Hogan and B. Piccarreta, “Interagency report on the status of international cybersecurity standardization for the internet of things (IoT),” 2018.

[68] OWASP, “OWASP Internet of Things Project.” [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Medical_Devices.

[69] “OWASP Top 10 vulnerabilidades.” [Online]. Available: https://www.owasp.org/images/thumb/7/79/OWASP_2018.

[70] ASSEMBLEIA DA REPÚBLICA, “Lei n.º 46/2018 Regime jurídico da segurança do ciberespaço,” pp. 4031–4037, 2018.

[71] J. Voas, R. Kuhn, P. Laplante, and S. Applebaum, “Internet of Things (IoT) Trust Concerns (Draft),” pp. 50–50, 2018.

[72] Shirey, “RFC 2828: Internet Security Glossary This,” *Internet Secur. Gloss.*, vol. 9, no. 2, pp. 1–212, 2000.

[73] OWASP, “Top IoT Vulnerabilities,” *OWASP*, 2016. [Online]. Available: https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.

[74] O. Digitasl, “A botnet Mirai está de volta e ameaça a internet. Saiba como se proteger!,” 2019. .

[75] G. Weidman, *Penetration Testing - A hands on introduction to Hacking*. 2014.

[76] CSO, “SQLi, XSS zero-days expose Belkin IoT devices, Android smartphones,” 2016. [Online]. Available: https://www.csoonline.com/article/3138935/sqli-xss-zero-days-expose-belkin-iot-devices-android-smartphones.html.

[77] W. N. Yard, “Manufacturer Usage Description Specification This - RFC8520,” pp. 1–60, 2019.

[78] NIST, “NATIONAL VULNERABILITY DATABASE.” [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

[79] D. Wood, N. Apthorpe, and N. Feamster, “Cleartext Data Transmissions in Consumer IoT Medical Devices,” 2018.

[80] HP, “The Insecurity of Network-Connected Printers : Executive Summary Sponsored by HP Independently conducted by Ponemon Institute LLC,” no. September, 2015.

[81] Internet Society, “IoT Security & Privacy Trust Framework v2.5,” pp. 1–6, 2017.

[82] IoT Security Foundation, “IoT Security Compliance Framework,” 2017.

[83] A. Mater and S. Universit, “Managing Challenges of Non Communicable Diseases during Pregnancy : An Innovative Approach Tesi in Sistemi Distribuiti,” 2017.

[84] A. Albataineh and I. Alsmadi, “IoT and the Risk of Internet Exposure: Risk Assessment Using Shodan Queries,” pp. 1–5, 2019.

[85] N. Davis, “Secure Software Development Life Cycle Processes,” no. July, 2013.