Seguridad de la información: un enfoque teórico

Trabajo de Fin de Grado

Grado en Ingeniería informática

01/01/2022

Jaime López Sánchez

_____

Ángel Luis Sánchez Lázaro

_____

Contenido

Resumen

El mundo es digital, y eso es una realidad. En apenas 20 años, hemos pasado de tener teléfonos en los que únicamente hacíamos llamadas, a tener dispositivos en los que almacenamos toda nuestra vida: nuestras conversaciones, apuntes, claves bancarias, entretenimiento, etc.
En el caso de las empresas, el cambio ha sido igual de rápido, ya que ninguna almacena sus datos en papel, tiene una sala dedicada exclusivamente a guardar archivadores o una herramienta por el estilo, ahora tenemos un servidor en algún lugar en el que podemos hacer estas acciones, o bien recurrir a la nube.
Pero esto trae un problema, y es que, ante un cambio tan rápido y repentino, la sociedad no se ha adaptado, y esto trae problemas que amenazan a los tres pilares básicos en los que se cimenta la seguridad de la información:

- Confidencialidad
- Integridad
- **Disponibilidad**

Muchas empresas hoy en día ni siquiera tienen un equipo dedicado a la seguridad de la información[1], sino que es el equipo de IT el que se encarga de hacer lo que pueden con esto.
Si nos fijamos en el artículo mencionado, el panorama es devastador. Únicamente un porcentaje ligeramente superior a la mitad de las empresas tiene un departamento dedicado a la ciberseguridad, y de ese porcentaje exclusivamente el 20% tiene un SOC (**C**entro de **O**peraciones de **S**eguridad en inglés), y es un servicio que se encarga de monitorizar alertas, filtrar falsos positivos, negativos o positivos verdaderos para que la carga de trabajo de los empleados finales sea menor)[2]dedicado para ella.
¿Qué problemas acarrea esto? Lo primero es que se suele dejar de lado para priorizar sus actividades asignadas, y a parte que un empleado tenga formación en IT, no quiere decir que sea adecuado para realizar el trabajo de un experto en Seguridad. El no tener un SOC supone que, aunque se tenga un departamento dedicado a esto, normalmente suele ser un equipo formado por menos de 5 personas, en ocasiones dedicado a empresas multinacionales, por lo que no tienen disponible un servicio 24x7 que monitorice alertas.

Además, tenemos otro problema grande que asumir. Incluso cuando hay un equipo dedicado a la ciberseguridad dentro de la empresa, muchas veces en caso de un incidente **no se sabe responder adecuadamente a la situación**. Teniendo en cuenta que las primeras horas son críticas, esto supone un escenario devastador, ya que hay que tener en cuenta que cuanto más tiempo pase mayor será el impacto:

- Reputacional
- Económico

[1] El 52% de las empresas cuenta con un departamento de ciberseguridad dedicado | Seguridad | IT Reseller

[2]https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia/2-uncategorised/5668-centro-de-operaciones-de-ciberseguridad-age.html

Teniendo en cuenta que el número de ciberataques no deja de aumentar[3], también lo hace el riesgo al que se somete cualquier empresa, ya sea grande o PYME.

Esto se puede deber también a que la educación tampoco está preparada para un cambio tan rápido. Sin ir más lejos, tomando como referencia las memorias de fin de grado de los alumnos de ingeniería informática, es bastante certero pensar que menos del 10% de estas se dedican a la ciberseguridad.
Y estoy de acuerdo en que en todas las asignaturas de la carrera (programación, sistemas distribuidos, administración de sistemas, etc.) hay un apartado que se centra en esto, pero aparte de que no es muy extenso, se suele dejar de lado por falta de tiempo, no dándole la importancia que en realidad tiene.
Esto supone una falta de conocimiento general tanto durante la vida académica, como luego en el mercado laboral, por lo que faltan muchísimos más profesionales cualificados en seguridad de los que hay disponibles en estos momentos.
Esto implica que, sin una debida protección de los activos, la entidad sea mucho más vulnerable a la pérdida de información sensible, interrupción de servicios, secuestro de servidores o equipos finales, junto con la pérdida económica que ello conlleva, sin olvidarnos del daño reputacional.

Objetivo del proyecto

El objetivo de este trabajo de fin de grado es ayudar a cambiar esta situación desde los cimientos, creando una supuesta arquitectura de red, que bien podría ser la de cualquier empresa que se dedique a dar un servicio a sus clientes.
Sobre esta arquitectura, se van a suponer distintos posibles ataques a los que podría ser sometida, y el cómo responder a ellos.
Es decir, cómo conseguir que el impacto en caso de ciberataque sobre la disponibilidad de los activos del negocio sea lo más bajo posible.

[3] https://economia3.com/2021/11/29/466826-ola-de-ciberataques-estas-son-las-grandes-empresas-golpeadas-por-los-hackers/

1. Estado del arte

Es necesario enseñar, y cuanto antes, cómo proteger la información de nuestras organizaciones. Porque si el incremento de ciberataques aumenta junto a la digitalización del mundo laboral (y en general también), ¿no sería lo suyo que la formación incrementase también para que cualquier persona, y no únicamente aquella con un trasfondo técnico supiera defenderse?

Es necesario que cualquier profesional relacionado con la informática, tenga unos mínimos conocimientos para identificar los riesgos de una organización, y si bien no ya mitigarlos porque para ello habrá profesionales específicos, al menos ser capaces de discernir qué hacer con ellos.

Para analizar la situación del panorama global en ciberseguridad, me voy a servir del siguiente informe de ISC2[4].

Esta compañía sin ánimo de lucro se encarga de concienciar a los profesionales y usuarios comunes, y sus certificaciones de seguridad son de las más reconocidas globalmente.

Bien, fijémonos en la siguiente tabla:

[4] [(ISC)² 2021 Cybersecurity Workforce Study (isc2.org)]

In addition to our global Cybersecurity Workforce Estimate of 4.19 million, our study provides 14 country-specific workforce estimates.

In 2021, we saw the most growth in

Germany
165% increase

Singapore
61% increase

United States
30% increase

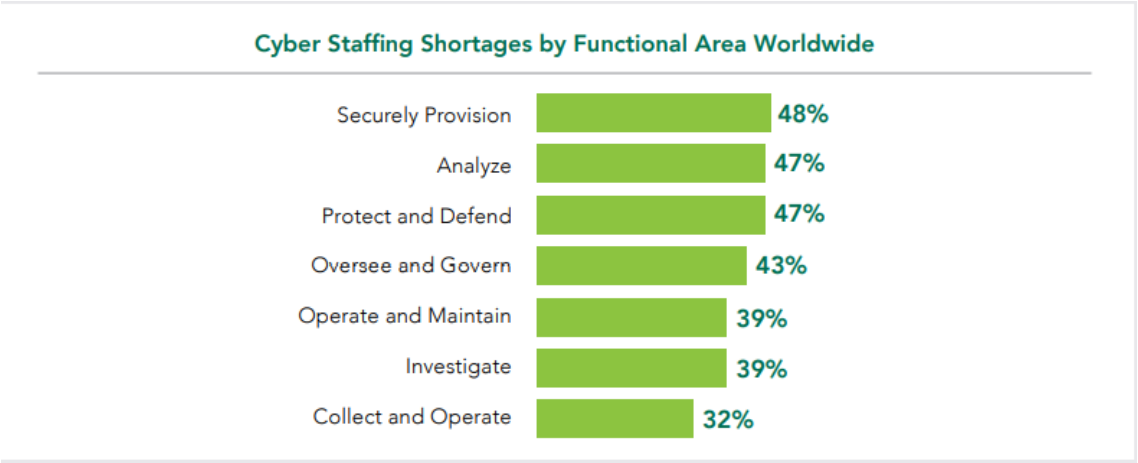
	2019	2020	2021
NA	**888,700**	**981,120**	**1,266,158**
U.S.	804,700	879,157	1,142,462
Canada	84,000	101,963	123,696
LATAM	**827,000**	**1,048,399**	**1,096,876**
Mexico	341,000	421,750	515,527
Brazil	486,000	626,650	581,349
EUROPE	**543,000**	**830,187**	**1,086,146**
U.K.	289,000	365,823	300,087
France	121,000	118,302	146,808
Germany	133,000	175,159	464,782
Ireland	N/A*	14,212	15,028
Spain	N/A*	122,284	124,336
Netherlands	N/A*	34,406	35,106
APAC	**544,000**	**625,265**	**743,075**
Australia	107,000	108,950	134,690
Japan	193,000	226,269	276,556
Singapore	43,000	57,765	92,744
South Korea	201,000	232,281	239,085
GLOBAL	**2,802,700**	**3,484,971**	**4,192,255**

Como podemos apreciar, España es de los países que menos crece en inversión en Seguridad, y no precisamente porque no seamos víctimas de ataques.
En los siguientes enlaces se puede conocer un poco más acerca de los ciberataques más sonados del último año:

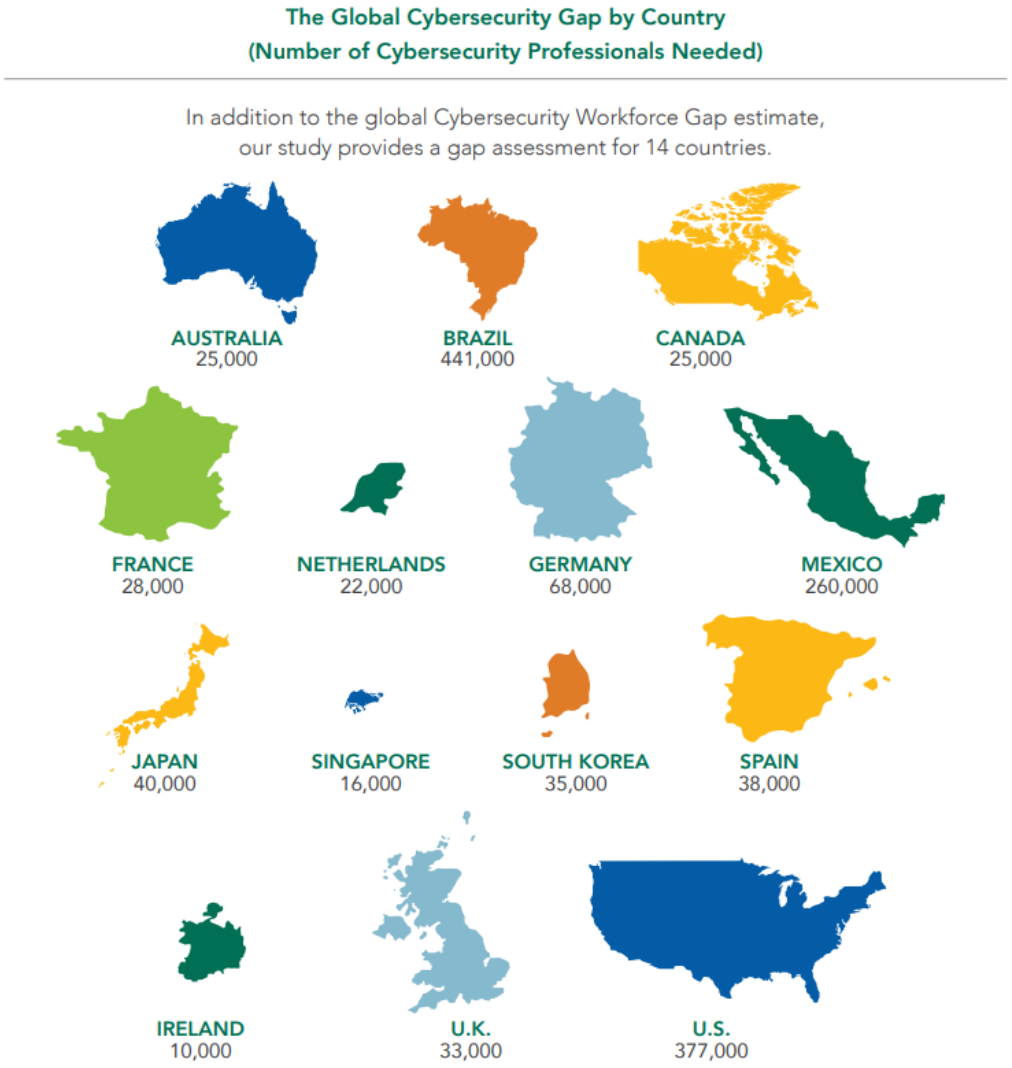
- El Ministerio de Trabajo sufre un nuevo ciberataque tres meses después del que afectó al SEPE (xataka.com)
- SegurCaixa Adeslas sufre un ataque ransomware que afecta a millones de usuarios - CyberSecurity News
- Adif sufre un ciberataque del que dice tener a salvo la seguridad de la red ferroviaria | Compañías | Cinco Días (elpais.com)

Como podemos ver, que no se invierta en ciberseguridad tiene consecuencias, y graves para todas las empresas, ya sean públicas o privadas.

Si avanzamos a la página 20 del informe de ISC2, analicemos los siguientes datos:

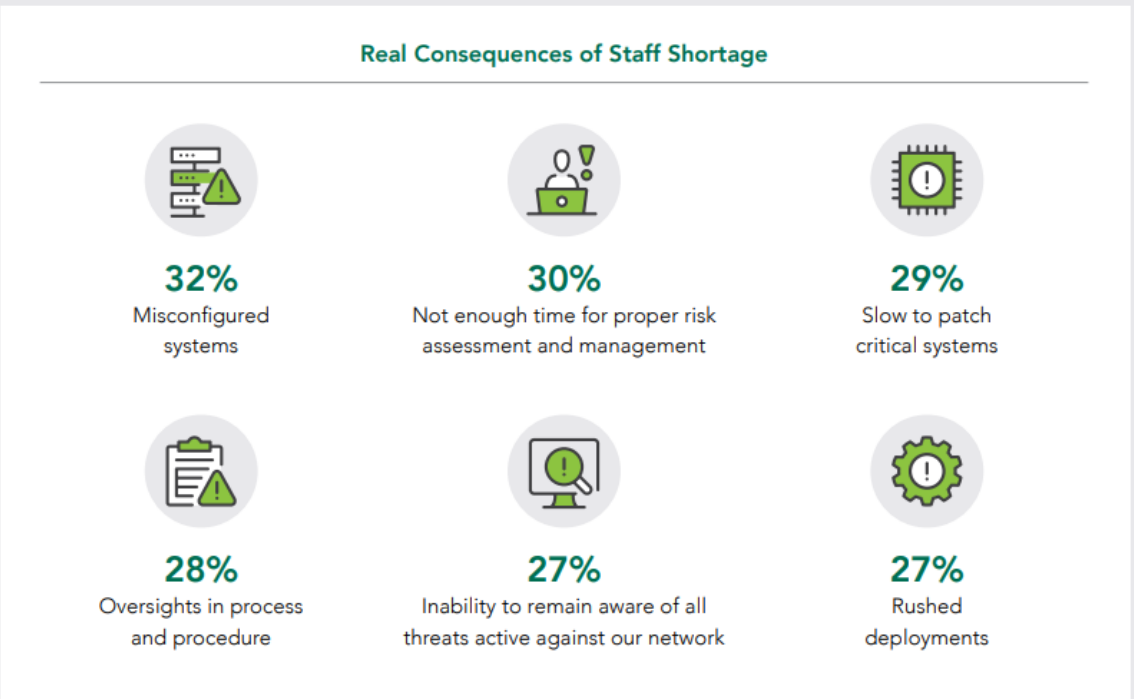


Falta prácticamente un 50% del personal necesario en algunas áreas para que todos los puestos de trabajo relacionados con la seguridad estén cubiertos. Teniendo en cuenta que este estudio se ha realizaado a nivel **global,** ¿por qué no se hace un mayor énfasis en formar a los estudiantes, para que haya más profesionales con verdaderas ganas de trabajar y mejorar el sector?



Según este estudio, en españa hacen falta alrededor de 38.000 puestos de trabajo, lo cual (y dado el índice de paro que tenemos en nuestro país), es realmente una pena que porque no se forme a profesionales en el sector no se acabe con este GAP al que nos enfrentamos.

Además, ¿qué supone que falte tal cantidad de personal para realizar estas acciones? En la siguiente imagen se pueden apreciar las consecuencias de esa falta de personal especializado.



Vamos a ver más en detalle qué puede implicar cada uno de estos puntos:

- Sistemas mal configurados: protocolos anticuados, configuraciones arcaicas (sobre todo en empresas que llevan con la misma infraestructura años) en la que no se tienen en cuenta mejores prácticas de seguridad, etc.
- No hay tiempo para un análisis de riesgos, y gestión de estos: imaginemos que vamos a desplegar un nuevo proyecto que va a ofrecer financiaciones a clientes a través de inteligencia artificial. Como no hay personal que analice los riesgos del proyecto, y que haga un plan de continuidad de negocio en el que se especifique qué hacer en caso de que se caiga el servidor, falle la inteligencia artificial, etc. Lo que se hace es desplegar y esperar que todo salga bien, lo que supone que en caso de incidencia, si este plan estuviera ya previsto se podría encontrar una solución quizás en menos de 24h, y no estar meses posiblemente de producción parada
- Lentitud a la hora de parchear sistemas críticos: hace justo unas semanas, más concretamente el 12/28/2021 tenemos el caso del Apache Log4j[5], CVE-2021-44832. Sin un departamento que esté pendiente de escenarios así, que además ocurren cada día prácticamente, ¿es IT el que se encarga de parchearlo? Si este grupo de trabajo ya tiene que realizar sus funciones cotidianas, posiblemente dejen esto de lado y esa vulnerabilidad quede abierta a exploits indefinidamente.

[5] Log4j y Log4Shell: La vulnerabilidad que en 3 días tuvo 60 ataques (newtral.es)

- No seguir procedimientos y políticas: lógicamente, para que no se sigan estos procedimientos primero es necesario haberlos creado, y en muchas empresas ni siquiera se ha llegado a este punto, lo cual hace este punto incluso más grave.
- Capacidad insuficiente de estar al tanto de las amenazas de red: es un caso similar al parcheado de sistemas, si no hay gente que se encargue de ello quedará como una tarea secundaria, y se realizará en algún momento, si hay tiempo para ello…
- Despliegues sin estar listos: si no se sigue unas prácticas de desarrollo de código seguro, un penetration testing del proyecto antes de salir a producción, etc. Lo raro sería que no se hayan aplicado malas prácticas, y que ese proyecto no sea vulnerable a distintos exploits de los que un ciberatacante pudiera beneficiarse.

2. Tecnologías- Conceptos

A lo largo del proyecto, se van a mencionar distintas tecnologías de seguridad que quiero primeramente definir aquí para su correcta comprensión.

2.1 Firewall

Un firewall es un dispositivo de seguridad de red que monitoriza el tráfico entrante y saliente, y según una serie de reglas especificadas en su configuración, es capaz de permitirlo o bloquearlo.

Estos dispositivos sirven para establecer una defensa entre redes internas y seguras, y redes externas no fiables como bien puede ser Internet.

2.2 DMZ

Son las siglas de zona desmilitarizada. Es una forma de organizar la arquitectura de red de una empresa que mejora la seguridad de dicha arquitectura. Estas VLANes se permite que sean accesibles desde Internet, normalmente se les añade para mayor seguridad un Firewall antes de la misma, separándolos de otra subred que normalmente estará detrás de otro firewall para permitir que únicamente el tráfico realmente deseado acceda a la red interna de la compañía.

2.3 PAM (Privileged Access manager)

Ayuda a crear un entorno robusto de gestión de accesos. Es decir, con esta herramienta aseguramos el acceso a un servidor, por ejemplo, permitiendo que únicamente a través de ella se obtengan permisos de administrador sobre el mismo.

A la hora de implementar una herramienta correcta y que vaya a realizar este funcionamiento correctamente, debería tener las siguientes características:

- Compatibilidad con los sistemas operativos más comunes: Windows, Linux, Unix, etc.
- Posibilidad de gestionar cuentas locales y de servicio
- Alta disponibilidad del servidor
- Gestión de credenciales: rotación de contraseñas, aprobación de permisos de acceso y registro de acciones para auditorías
- Como comentaba anteriormente, la posibilidad de acceder a ciertos entornos mediante RDP[6] que no exponen la contraseña del usuario (esto se hace con un almacén de contraseñas que suelen tener estas herramientas)
- Reglas que alerten si se crean cuentas/permisos sin consentimiento previo
- Multi factor de autenticación y single sign on (el single sign on sirve para que se unifiquen las cuentas de los servicios de una empresa, y únicamente con un usuario y contraseña el usuario pueda acceder a varios servicios)
- Incluso los más avanzados pueden estar integrados con un SIEM o SOC

Como ejemplo, adjunto Cyberark[7].

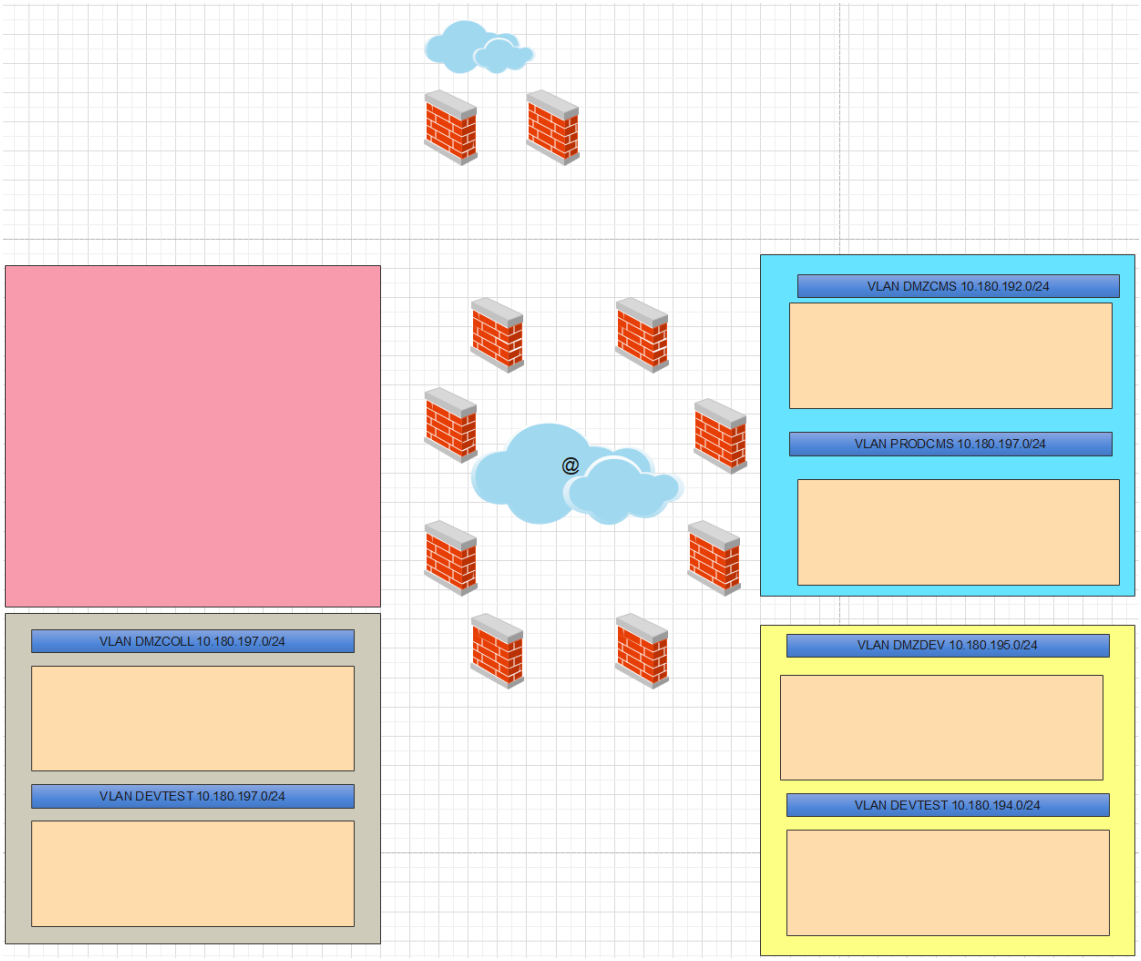
3. Diseño de red

a. Diagrama de red

Se va a crear un modelo que podría servir como la arquitectura de red de una empresa, donde estarían alojados todos sus servidores, equipos y subredes. A continuación, se va a hacer una descripción de alto nivel del diagrama de red de nuestra empresa A.

[6] Remote desktop protocol: es un protocolo de red que sirve para conectarse a otra máquina o servidor en remoto

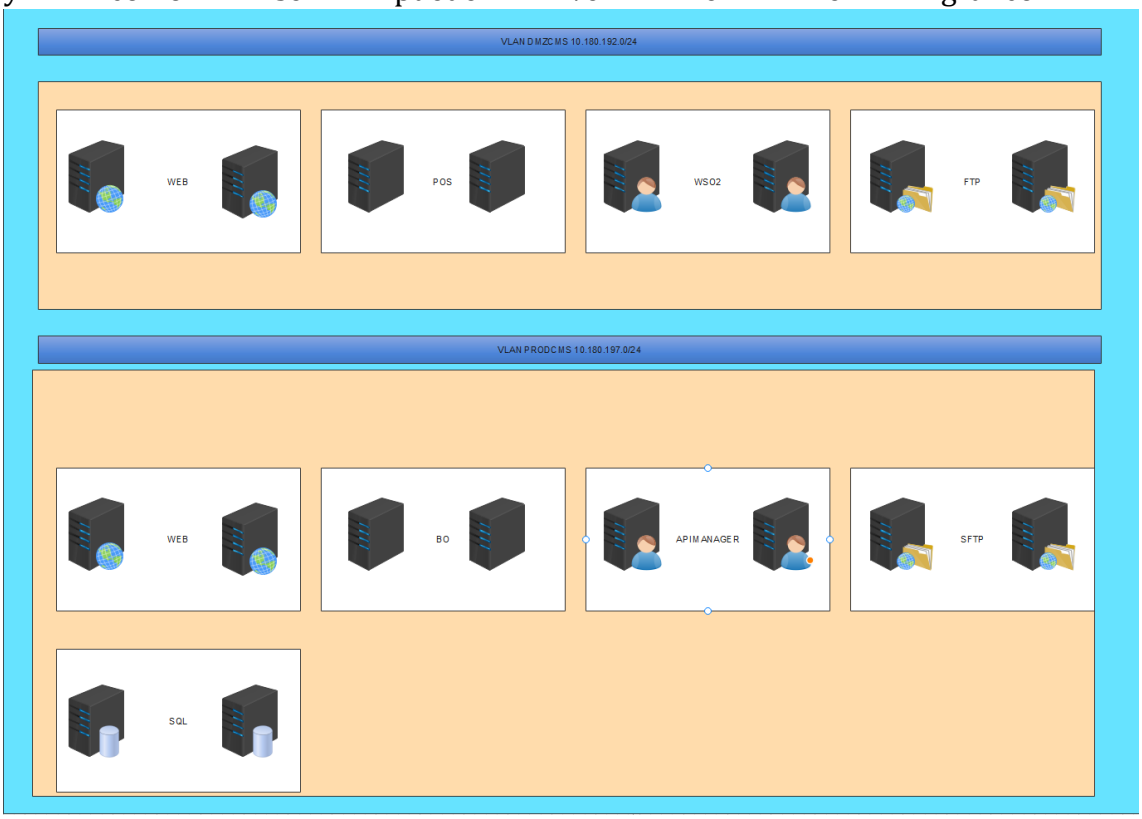
[7] https://www.cyberark.com/es/



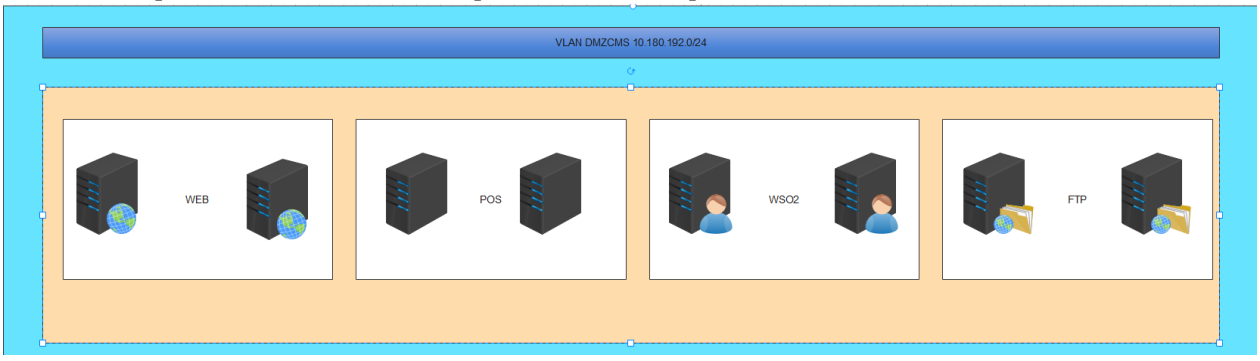
Estos distintos entornos serán explicados poco a poco a lo largo del documento.

Dentro de la arquitectura de red existen 4 grandes zonas, separadas por diferentes capas de firewall.

- ***Zona de Producción.*** Que se encuentra a su vez dividida en dos VLANes, tal y como se puede ver en el gráfico.

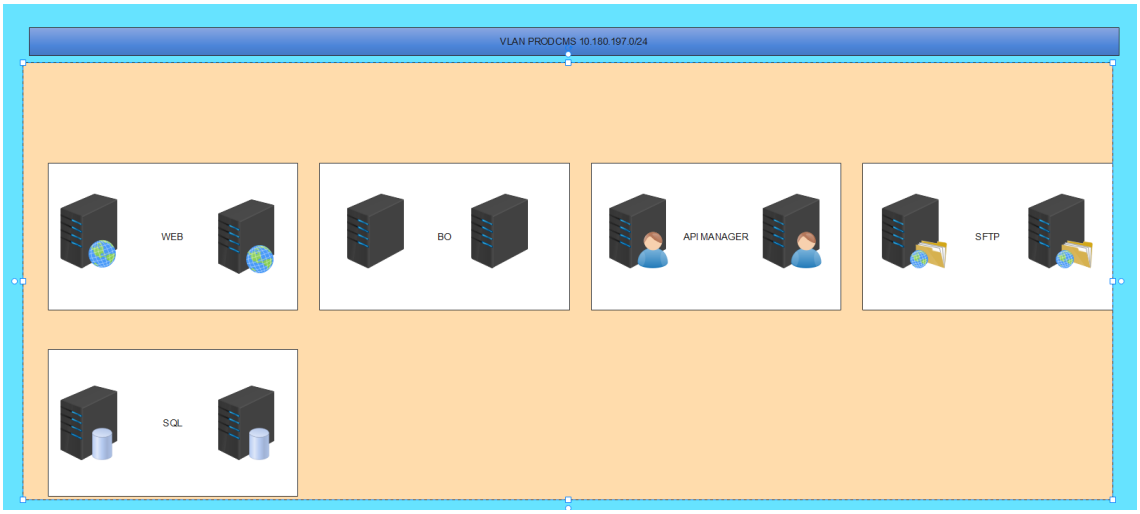


- VLAN DMZCMS. Esta VLAN es la VLAN que tiene los servicios de Frontend, es decir, aquellos servicios que están publicados en Internet:



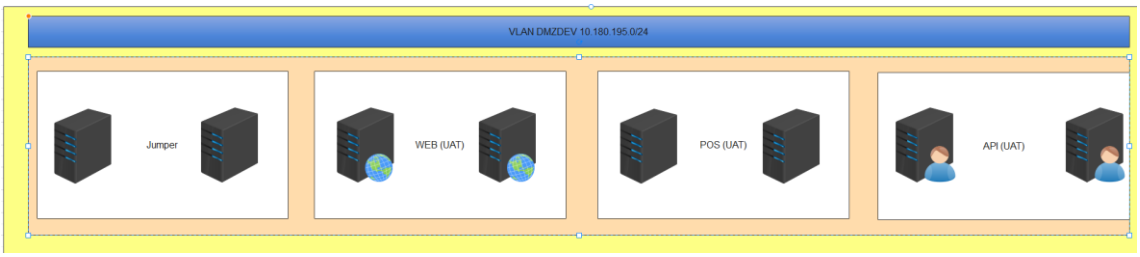
  - ***Web Corporativa.***
  - ***Punto de venta.*** Es donde los comercios acceden para crear las operaciones con los clientes.
  - ***API.*** Donde se encuentran publicados los servicios que consumen las diferentes aplicaciones periféricas, necesarias para realizar la actividad de la empresa
  - ***SFTP.*** Utilizado para el intercambio de archivos con entidades externas.

- VLAN PRODCMS. Esta VLAN es la VLAN que tiene los servicios de Backend y BBDD, es decir, aquellos servicios que no están publicados en Internet y que albergan tanto las BBDDs como los accesos necesarios para la correcta gestión de la actividad de la empresa así como, intercambio de archivos/ficheros internos. Los elementos que lo componen son:

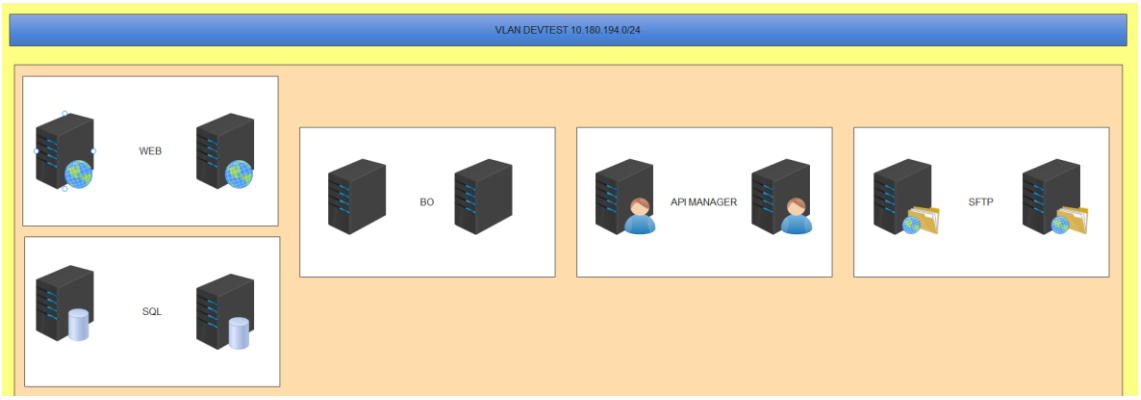


  - ***BBDD de la Web Corporativa***
  - ***BBDDs SQL***
  - ***BO:*** es un filesystem que almacena ficheros y es usado por algunas áreas de negocio. También funciona como almacén intermedio en el que compartir los archivos con clientes y externos
  - ***API:*** entorno de backend de la API
  - ***SFTP:*** entorno sftp de backend

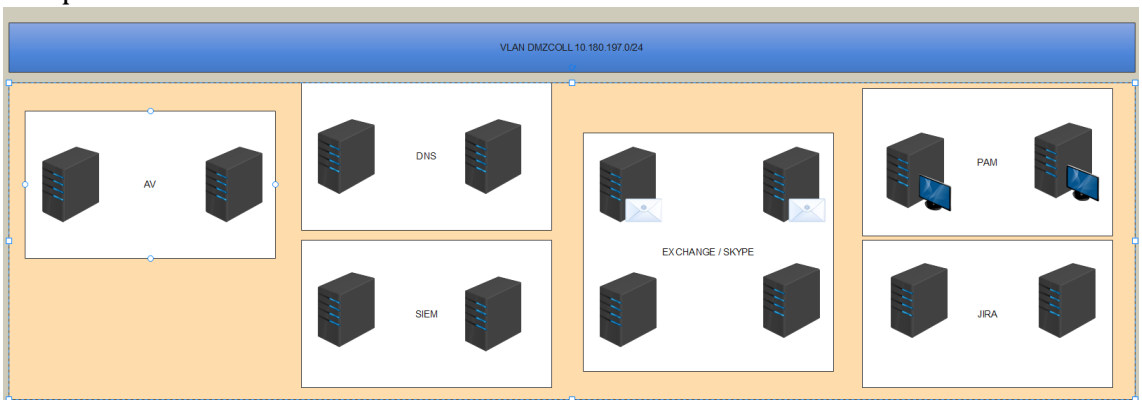
- ***Zona de preproducción: dividida también en dos VLANes***
  - ***VLAN DMZDEV:*** tiene los servicios de Front de desarrollo, simulando el entorno de Producción.



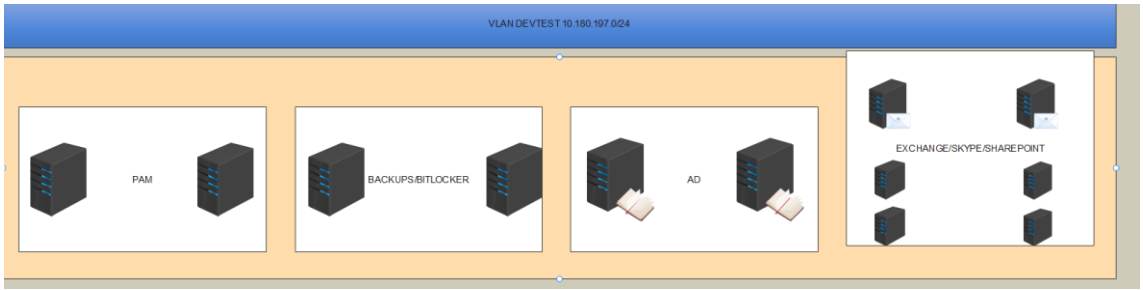
    - **Jumper**: este servidor es el empleado por el PAM. Permite acceder a un entorno remoto de administración segura.
  - **VLAN DEVTEST*:*** esta VLAN tiene los servicios de backend y BBDD, pero además es una réplica perfecta del entorno de producción



- ***Zona de colaboración.*** En esta zona se encuentran las herramientas colaborativas y de seguridad necesarias para el correcto funcionamiento de la compañía. Se encuentra a su vez dividida en dos VLANes.

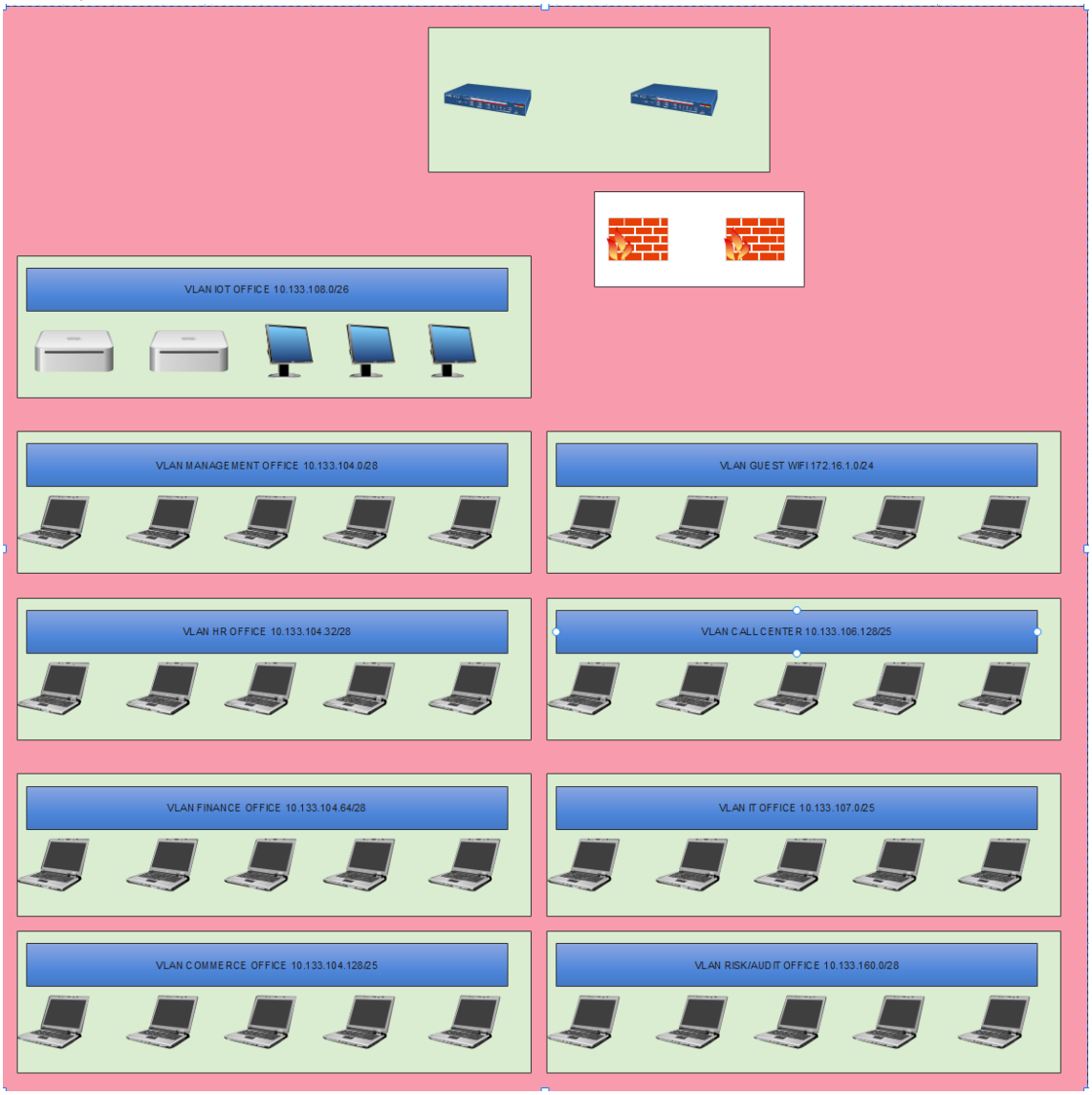


  - VLAN DMZCOLL: tiene los servicios colaborativos del front end
    - ***DNS:*** *resolución de dominios*
    - ***Servicios de correo y Skype for Business (vamos a imaginar que no están usando en esta compañía una solución en cloud como podría ser O365)***
    - ***Servicios de DLP y AV***
    - ***Servicios de SIEM***
    - ***Jira***
    - ***PAM***
  - VLAN COLLCMS: tiene los servicios de Backend asociadas a las herramientas



    - Servicios de autenticación: AD
    - Servicios de Correo, Skype for Business y Sharepoint
    - BBDD de la solución PAM
    - BBDD del DLP y el AV

- **HQ.** Esta zona, es la distribución de la red de Área Local de las oficinas centrales de la compañía. El diseño está orientado a asignar una VLAN de red en función de la membresía del usuario a su área/departamento. Un usuario del departamento de Commerce será asignado a la VLAN del departamento de Commerce, tal y como se puede revisar en el gráfico adjunto.



4. Clasificación de activos

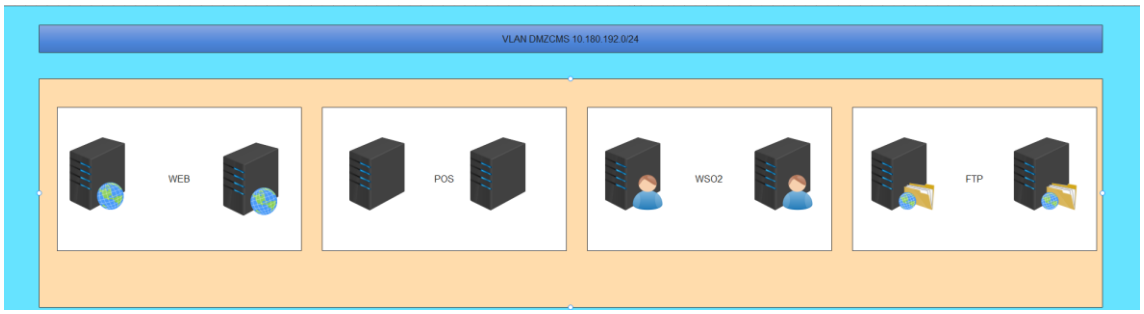
A la hora de realizar una evaluación de activos que permita establecer un claro criterio que gobierne la recuperación ante un desastre, es necesario hacer un análisis basado en dos criterios: continuidad del negocio y otro basado en la operatividad de la compañía.

a. Análisis de activos basada en negocio

i. Servidores con prioridad de recuperación crítica

Desde el punto de vista de negocio, existen una serie de sistemas cuya recuperación debe ser inmediata con objeto de garantizar la continuidad de este.

Entorno de Producción. VLAN DMZCMS

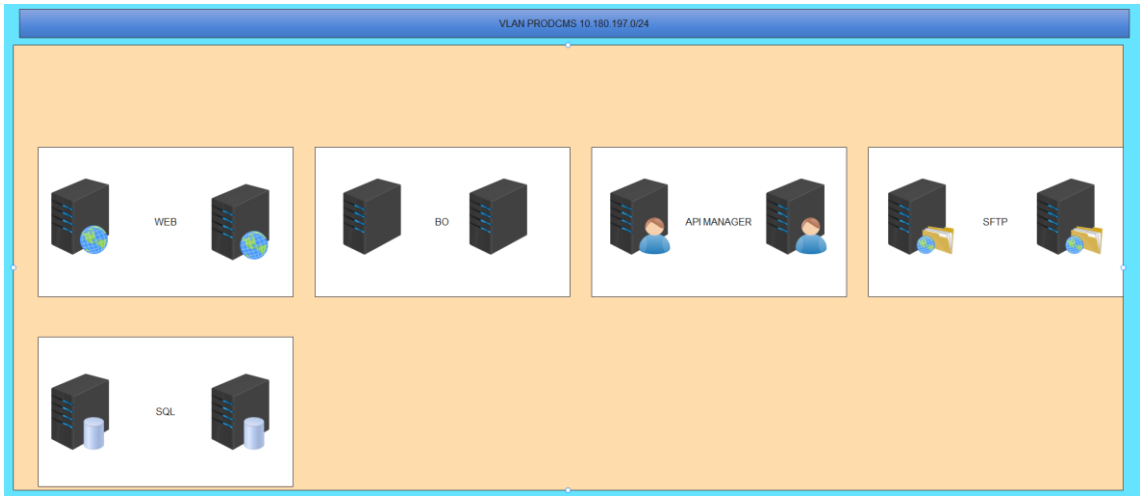


Punto de venta: ambos servidores contienen la web a la que acceden los negocios a los que nuestra empresa presta servicios para que ellos gestionen las operaciones con sus clientes. El segundo servidor, al igual que en el resto, está para garantizar la alta disponibilidad en caso de caída del primero. *Uno de ellos debe ser considerado crítico.*

API: estos servidores contienen la API. A través de ella se produce la comunicación con los elementos externos que realizan procesos críticos para el customer onboarding y merchant onboarding, además de servir de enlace con diferentes hubs de financiación. *Uno de ellos debe ser considerado crítico.*

SFTP: estos servidores sirven para enviar/recibir ficheros a externos. *Uno de ellos debe ser considerado crítico.*

Entorno de Producción. VLAN PRODCMS



En este entorno, existen los siguientes servidores:

BO: es el servidor de inteligencia, donde se decidirá si se aprueban o deniegan operaciones con clientes (esto puede ser llevado a cabo por inteligencia artificial o

por una persona que esté detrás). Dado que las operaciones del POS se replican aquí, si este servidor se cae el servicio entero no podrá continuar, por lo tanto *uno de ellos debe ser considerado crítico.*

Base de datos: se guardan los datos. *Uno de ellos debe ser considerado crítico.*

API: servidor de administración de la API. *Uno de ellos debe ser considerado crítico.*

SFTP: estos servidores sirven para enviar/recibir ficheros a externos. *Uno de ellos debe ser considerado crítico.*

ii. Servidores con prioridad de recuperación alta

Existen servidores que albergan funcionalidades de negocio que también se consideran claves para el buen funcionamiento de la compañía, pero que pueden ser consideradas en un orden secundario de prioridad a la hora de recuperar los mismos. En este caso, básicamente estaríamos hablando de la web corporativa, dado que vamos a suponer que en nuestra empresa la web únicamente tiene fines de marketing o blog de noticias.

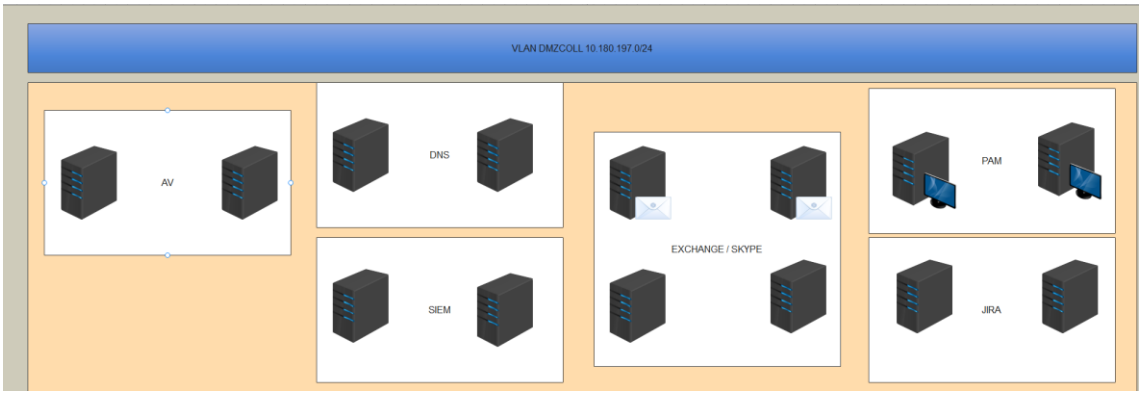
WEB: alberga la web de la compañía.

b. Análisis de activos basada en operabilidad

Adicionalmente a los activos que son críticos para mantener la continuidad de negocio es necesario identificar los activos que son básicos para mantener una actividad mínima que garantice el servicio a los clientes y a los propios empleados.

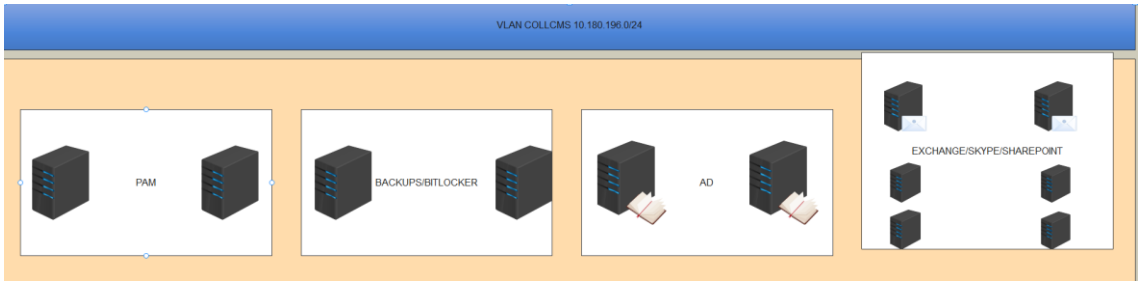
i. Servidores con prioridad de recuperación crítica

Entorno de Colaboración. VLAN DMZCOLL



DNS: realiza el rol de DNS externo, que permite la resolución interna/externa de nombres (solo es necesario que esté activo uno de los dos)

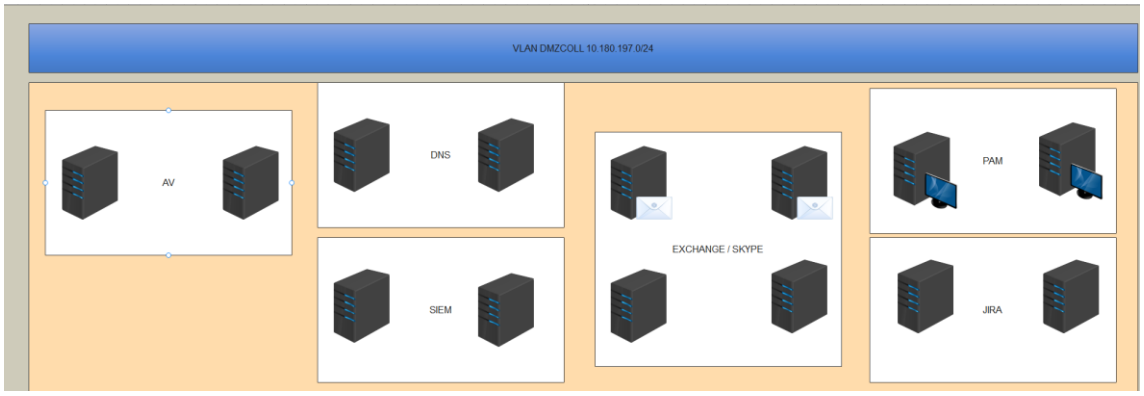
Entorno de Colaboración. VLAN COLLCMS



AD: controlador del dominio.

ii. Servidores con prioridad de recuperación Alta

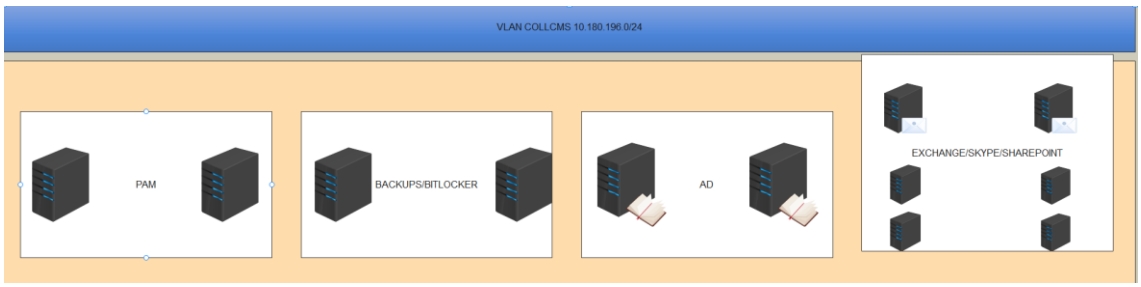
Entorno de Colaboración. VLAN DMZCOLL



SKYPE/EXCHANGE:

- **MP01**: tiene un rol de proxy para las aplicaciones de Outlook y Skype for business
- **MP02**: espejo del anterior, para garantizar alta disponibilidad
- **MS01**: servidor para el correo electrónico
- **MS02**: backup del anterior

Entorno de Colaboración. VLAN COLLCMS



SKYPE/EXCHANGE:

- **MB01**: mailbox de Outlook
- **MB02**: mailbox de Outlook

- **MSF01**: servidor para el Skype
- **MSF02**
- **MSH01**: Sharepoint*
- **MSH02**

5. Portátiles

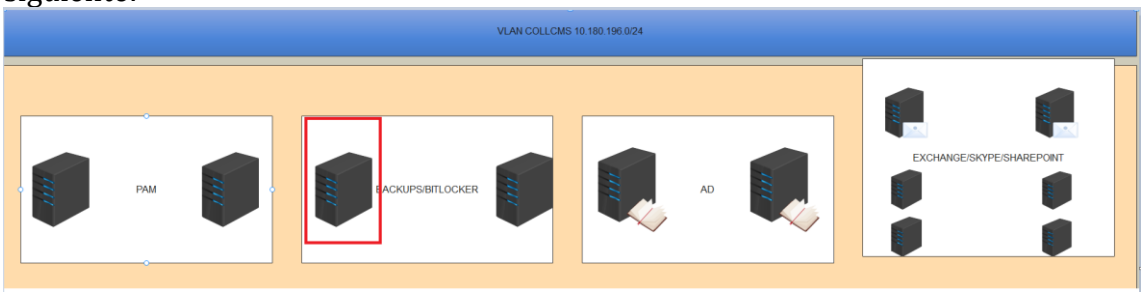
Para garantizar la plena operatividad de la compañía es necesario considerar la recuperación de portátiles en el caso de que se produzca un ciberataque que ponga en riesgo la integridad, confidencialidad o disponibilidad de los equipos. Éste sería el caso de un ransomware asociado a la encriptación del dispositivo portátil.

Del mapa de red se puede observar la distribución a nivel de red de las oficinas. De esta manera cada dispositivo se conecta a la VLAN propia de su departamento, estando deshabilitado la opción de que un ransomware inteligente pueda saltar entre diferentes redes y proceder a una encriptación global de todos los portátiles en todas las subredes.

Aun así, hay que contemplar la posibilidad de que el principal vector de entrada de un ransomware sea el correo electrónico, por tanto, ante un envío masivo sería razonable considerar afectación en diferentes subredes e incluso una indisponibilidad masiva de ordenadores debido a un encriptado, es por ello que hay que establecer un diseño asociado a la configuración del mínimo número de ordenadores necesario para garantizar el servicio.

3.1.2 Recuperación de datos en portátiles

Es necesario contemplar un escenario en con la posibilidad de la recuperación de datos. Para ello es necesario garantizar la disponibilidad del servidor de backup siguiente:



6. Vectores de ataque: portátiles

Tal y como se encuentra diseñada la seguridad de los elementos portátiles existen varios vectores de entrada de malware dentro de la infraestructura técnica:

- Periféricos. A través de la conexión de periféricos mediante puertos USB/USB-C. Cuando existe una conexión de un dispositivo: ratón, teclado o cualquier elemento que requiere un intercambio de conexión entre el laptop y el dispositivo, generando la descarga en el laptop de firmware, software o archivos.

- Navegación. Mediante navegación a infraestructuras externas o internas que hayan sido comprometidas.

- Correo. Mediante correo electrónico, durante la recepción y posterior.

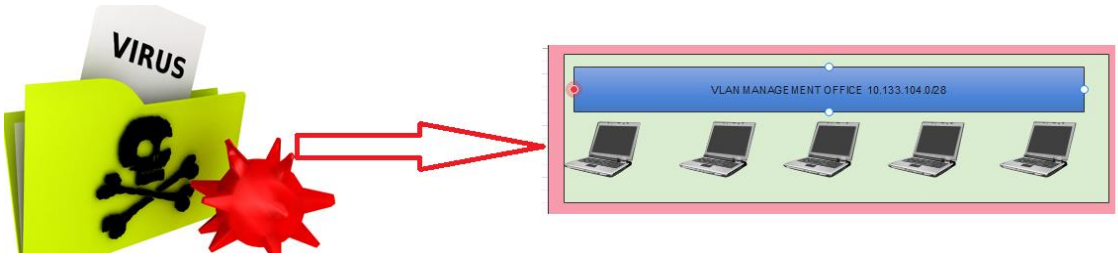
- Interconexión a Redes.

4.1Periféricos

Si se produce un ciberataque cuyo vector de entrada es la conexión de un periférico a través de los puertos USB o USB-C, la transmisión del malware se produce mediante la instalación del firmware del periférico a través del cual se introduce bien un malware operativo o bien una parte sustancial del mismo que constituye la piedra angular para desentrañar el ataque.

Paso I - Infección

Tal y como se ha indicado, la infección se produce por la instalación de malware en el ordenador afectado.



Una vez que el malware se encuentra alojado en el portátil, existen diferentes variantes:

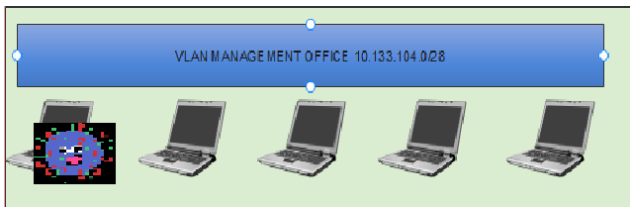
- Si el malware no es sofisticado su objetivo es tratar de escalar privilegios dentro del ordenador para tomar el control del mismo, desactivar los elementos de seguridad reconocidos: antivirus, antimalware, así como, prepararse para la posible propagación y posterior encriptado de los sistemas.

- Si el malware es sofisticado su objetivo es establecer una cabeza de puente para seguir descargando malware adicional que permita establecer un set de herramientas que le permita profundizar dentro de la arquitectura de sistemas de la compañía.

Nota: Salvo en el caso de los malwares más sencillos que sí que generan procesos perceptibles para el usuario (se abre la calculadora de Windows, aparece un pantallazo azul, desconexión puntual de la pantalla), habitualmente solo se puede advertir una anomalía a nivel de ejecución de procesos. Al revisar los procesos que se están ejecutando se puede observar un nuevo proceso con un nombre genérico como print.exe o similar.

Paso II – Toma de Control

El siguiente paso, una vez que el malware se ha instalado en el ordenador procedente del periférico, es la toma de control del equipo mediante el escalado de privilegios.



Dicho escalado se puede hacer por:

- Existencia de una vulnerabilidad bien sea a nivel de Sistema Operativo bien sea a nivel de otras aplicaciones que permita escalar privilegios a permisos de administrador.

- Rotura de credenciales/hash almacenadas de manera local. El malware encuentra la manera de romper protocolos de intercambio de credenciales y hace el escalado de privilegios.

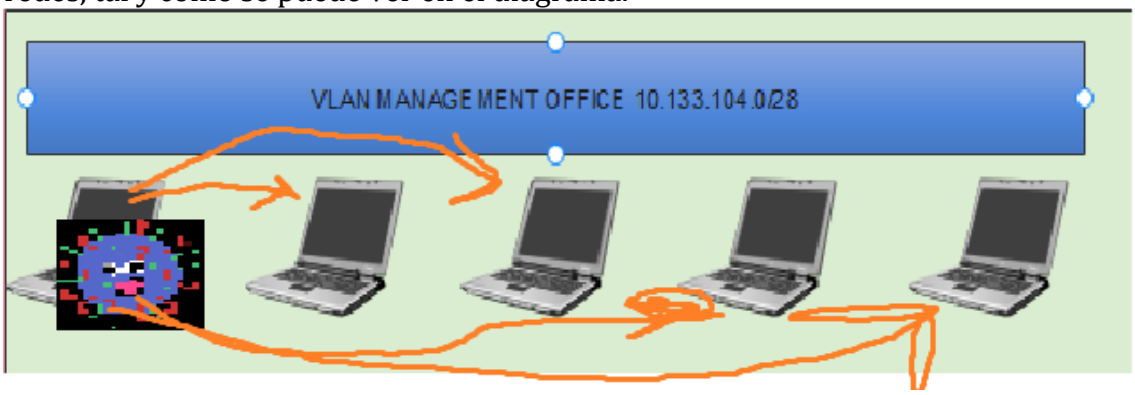
Una vez que ha tomado el control del equipo, el malware puede realizar las siguientes acciones:

- Deshabilita todas las herramientas de seguridad instaladas de manera local, en este caso sería el agente del DLP, el agente de antimalware Symantec, el firewall de Windows o el agente del SIEM entre otros.

- Procede a continuar con la infección mediante la ejecución de diferentes comandos y programas.

Paso III (i) –Pivotado

Si el objetivo del malware es generar el mayor daño posible a la compañía, sin tener como objeto el robo de datos, el proceso siguiente es el del pivotado, es decir el salto de un laptop a otro laptop situado en la misma red, así como, la exploración a otras redes, tal y como se puede ver en el diagrama.



Por configuración de la seguridad, no será posible pivotar entre las diferentes redes, ¿qué ocurre entonces?

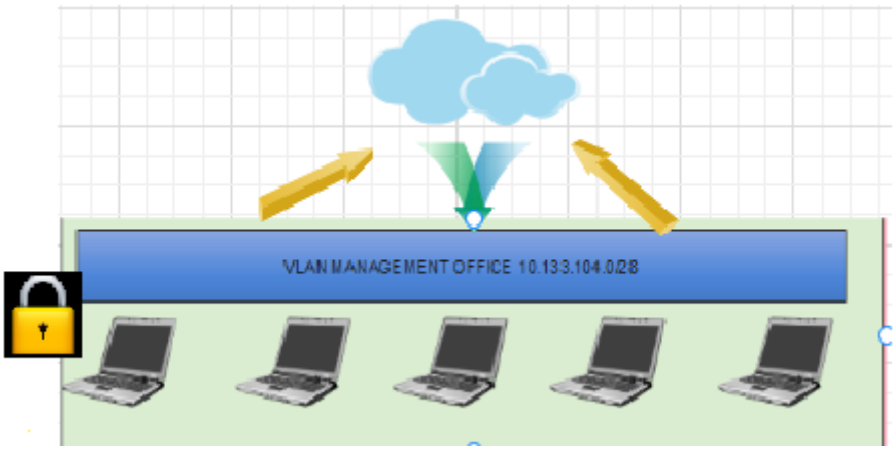
Paso III (i.a) –Fallo en la pivotación

Al no poder pivotar hacia más ordenadores o incluso servidores, los ordenadores de una misma red quedarían comprometidos y pendientes de ser encriptados. Si el malware tiene como propósito la encriptación/secuestro del mayor número de equipos posibles, la orden de encriptar los equipos se puede generar de dos maneras:

- El malware hace una llamada de callback hacia un recurso en Internet alcanzable con una dirección IP pública. Se vería tráfico de navegación web desde el ordenador encriptado hacia Internet. En la respuesta se da la orden de encriptación.

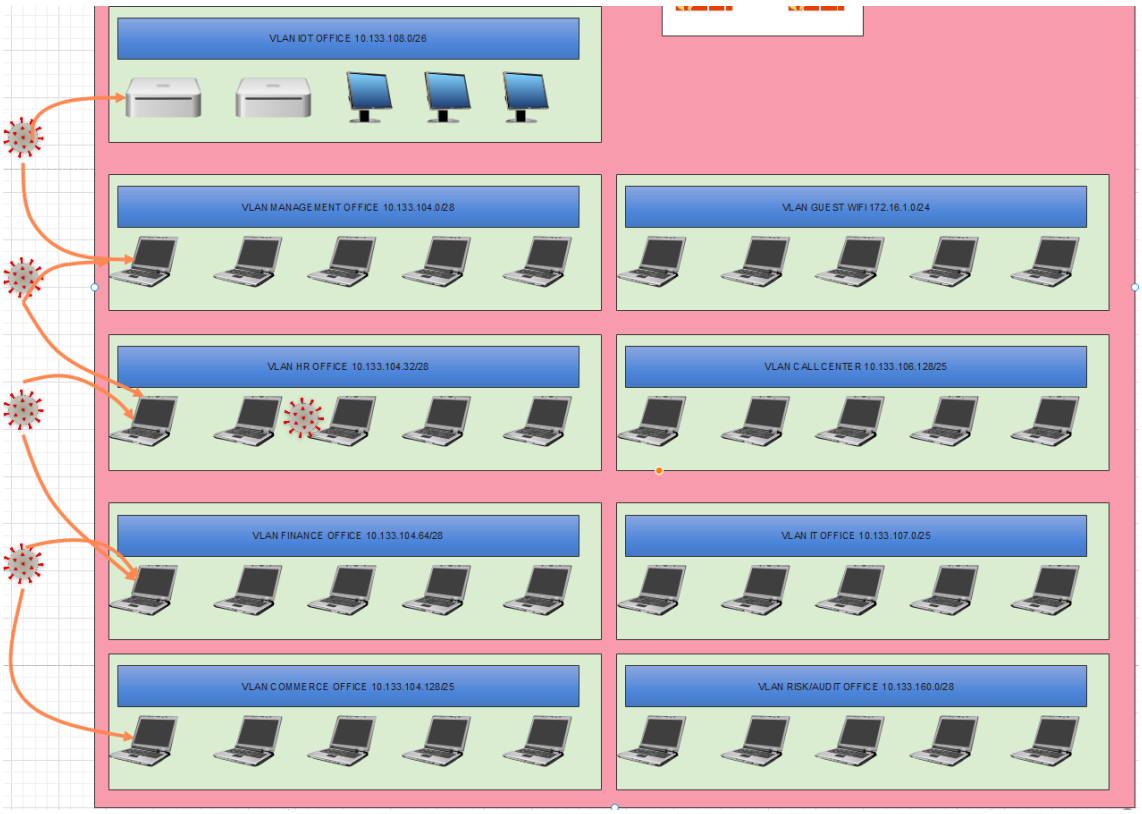
- El malware hace una llamada de callback pero la navegación hacia el recurso está cortado, por tanto se activaría un timer empotrado en el programa.

Llegado a 0 ese temporizador el dispositivo infectado se procedería a encriptar.



Paso III (i.b) –Éxito en la pivotación

Si el malware, una vez infectado el dispositivo, puede pivotar no solo dentro de la red, sino también entre diferentes redes, el grado de afectación se extenderá a todas las redes del HQ y con un posible impacto a los servidores alojados en los Datacenters.



Si el malware, mediante la exploración de red, puede continuar propagándose dentro de la red existen muchas más opciones de que las llamadas de callback resulten exitosas. Estas llamadas de callback tratarán de que uno o varios

dispositivos comprometidos puedan bajarse de sitios de Internet otros malwares adicionales que permitan añadir más capacidades:

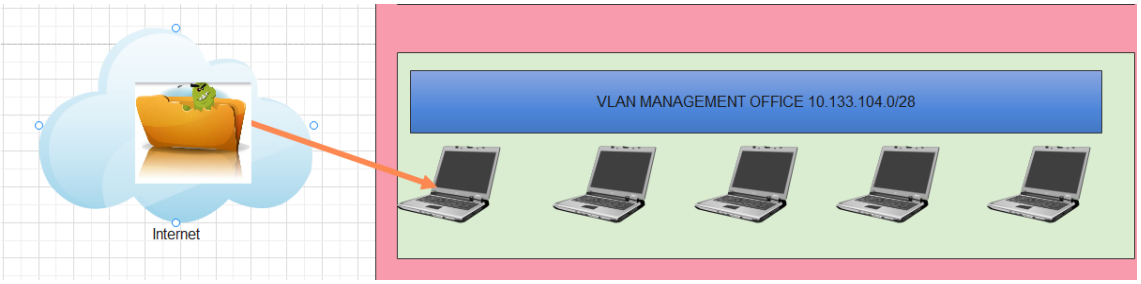
- Malware con capacidad para saltar hasta el directorio activo y tratar de conseguir un usuario de dominio.
- Malware con capacidad para saltar hasta las Bases de Datos, robar información y encriptarla.
- Malware con capacidad para saltar a cualquier tipo de servidor y encriptar los sitemas operativos.
- Malware con capacidad para saltar a las consolas de administración de las máquinas virtuales y de los sistemas de Backup dentro del Datacenter.

4.2 Navegación

La infección se produce por la descarga de un recurso almacenado en Internet al que se accede mediante navegación.

Paso I - Infección

Tal y como se ha indicado, el usuario accede a un recurso público, una web o similar, que esconde parte o el total de un malware.



La bajada del archivo y su posterior instalación es la concatenación de dos vulnerabilidades

- Vulnerabilidad asociada al filtrado de contenidos de navegación. El filtrado de contenidos es incapaz de identificar que el dominio web o el tráfico de navegación esconde un contenido malicioso.

- Vulnerabilidad asociada a los permisos de instalación del Sistema Operativo. Existe una debilidad en los permisos que permite la autoinstalación del archivo descargado.

Paso II- Callback

Dado que el malware ha descubierto una vulnerabilidad en el filtrado de contenido, esa vulnerabilidad es usada para realizar diferentes callbacks que permiten la descarga de diferentes malwares con diferentes funcionalidades desde el ordenador comprometido.

Paso III–Pivotación

Dado que se aprovecha de una vulnerabilidad en la navegación web, es fácil, la pivotación no solo dentro de la red, sino también a otras redes. La peculiaridad de este tipo de ataques es que se trata de tener siempre una puerta trasera , es el equipo infectado original.

Paso IV–Extracción de información/Posible Encriptación
Una vez que se encuentra pivotando entre los diferentes sistemas, se puede mantener el backdoor para tratar de extraer a partir de aquí toda la información posible y con objeto de eliminar todo rastro se procede finalmente a realizar la encriptación de todos los sistemas comprometidos.

4.3 Correo

La infección por correo es el principal vector de ataque, así como, el más utilizado con el objeto de comprometer la seguridad de la mayoría de las empresas (recordemos que el eslabón más débil siempre va a ser el humano). En ese sentido, existen 3 barreras de defensa con objeto de tratar de evitar que un laptop se infecte:

- El antispam que protege la entrada de correo y que descarta aquellos correos que son etiquetados como maliciosos. Aunque se eliminan buena parte de los correos, los más sofisticados suelen pasar el filtro antispam y llegan a los servidores de correo electrónico Exchange. En muchas ocasiones, el antispam es capaz de cortar los correos con adjuntos, pero los correos que tienen embebidos un enlace son incapaces de identificarlos/etiquetarlos.

- La siguiente barrera de protección está relacionada con el EDR, es decir, el sistema de protección desplegado en los dispositivos finales que escanea analiza y bloquea los archivos maliciosos que pueden estar escondidos en los correos. Existen dos opciones cuando un correo con un malware pasa la primera barrera del antispam

    - El antispam ya ha eliminado el adjunto del correo pero queda el enlace.
    - El EDR bloquea el archivo adjunto que no se ha eliminado por el antispam.

- En el caso de que ni el antispam ni el EDR consigan bloquear el correo, la última barrera de defensa es el bastionado de los equipos. Este bastionado se encarga de evitar la autoinstalación de los archivos cuando el usuario hace click el adjunto del correo.

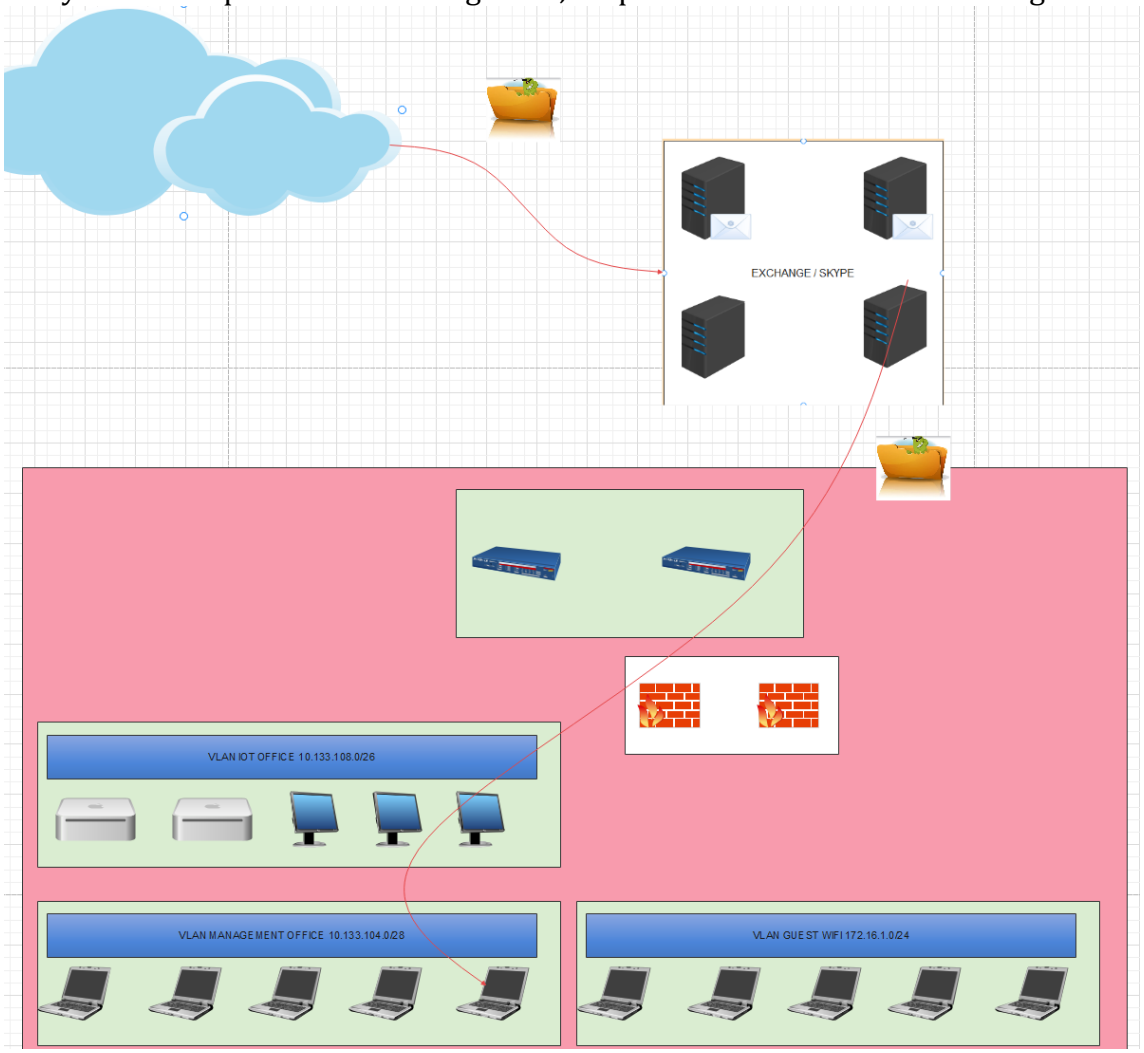
A pesar de las barreras de defensa, existen opciones de que se produzca la infección bien sea por:

- El malware es tan nuevo que las firmas del antispam y del EDR no son capaces de identificarlo.

- El malware se aprovecha de una vulnerabilidad existente en el bastionado o en el SO y se instala.

Paso I - Infección

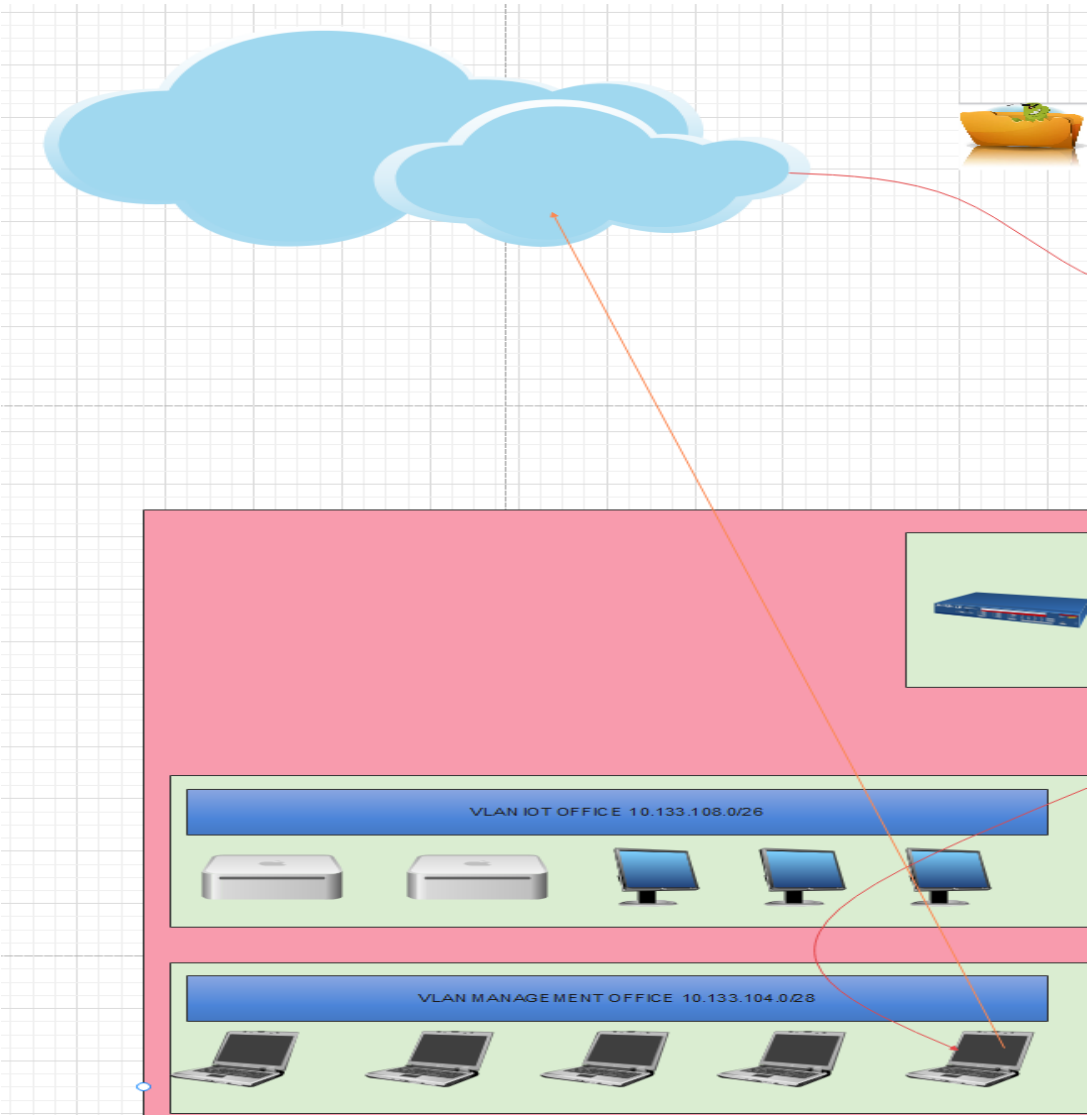
Tal y como se puede ver en el gráfico, el proceso de infección es el siguiente.



El correo con el archivo malicioso llega a la plataforma de Exchange. El agente de Outlook se sincroniza con Exchange y en el momento en el que el correo con el malware llega a Exchange, el agente de Outlook actualiza en local el correo, recibiéndose en el laptop del usuario. Si el usuario hace click en el correo, se abre. El problema radica en el momento en el que el usuario hace un click al archivo malicioso, una vez hecho el click se procede a realizar la instalación del malware, siempre y cuando el bastionado no lo haya parado, en ese momento el ordenador se encuentra comprometido

Paso II- Callback

En este caso existe una última línea de defensa, basada en el callback, que debe realizar el software atacante. Esa última línea de defensa es el firewall perimetral.



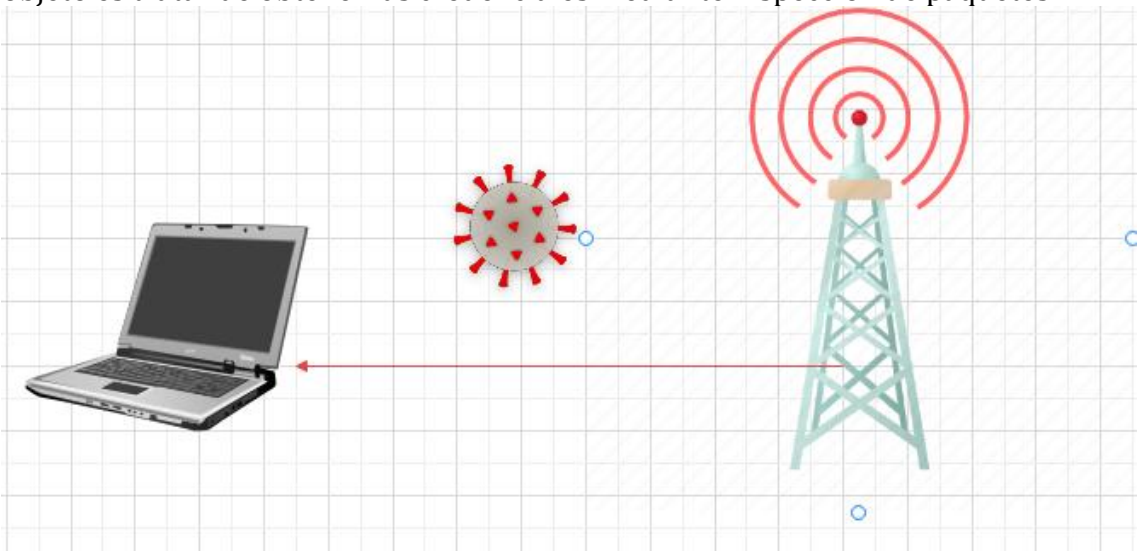
En el caso de que el callback tenga éxito y el firewall sea incapaz de parar la conexión, se produce la infección efectiva del ordenador y puede ejecutar los siguientes pasos vistos en los otros vectores de entrada, como pueden ser la pivotación, extracción de Información, así como, encriptación de sistemas.

Paso III–Pivotación

Dado que se aprovecha de una vulnerabilidad en la navegación web, es fácil, la pivotación no solo dentro de la red, sino también a otras redes, incluido el DataCenter. La peculiaridad de este tipo de ataques es que se trata de tener siempre una puerta trasera, es el equipo infectado original.

4.4 Interconexión a Redes

En este caso el vector de entrada se produce por la simulación de un hotspot corporativo o de una conexión wifi (aeropuerto, restaurante, etc.). En este caso el objeto es tratar de obtener las credenciales mediante inspección de paquetes.



Paso I - Infección

Tal y como se ha indicado, el usuario accede a un recurso público, que puede ser un hotspot Wifi de un aeropuerto, tienda, cadena de comida rápida, etc o bien puede ser mediante la simulación de un hotspot que trata de atraer la atención del usuario que se quiere conectar. Existen dos opciones desde el punto de vista del hacking:

- El hotspot donde el usuario se quiere conectar ha sido vulnerado previamente, la compañía que ofrece el hotspot no es consciente de dicha vulnerabilidad.
- El hotspot está hecho con un objetivo malicioso.

El objetivo del ataque es, usando el PC del usuario que se ha conectado al hotspot, fundamentalmente la intención es extraer credenciales, información, etcétera para tratar de ampliar el alcance del ciberataque.

7. Vectores de Ataque: Servidores

Tal y como se ha supuesto la seguridad de esta empresa, existen los siguientes vectores de ataque asociados con la seguridad:

- Ataque por Denegación de Servicio. Al tener servicios publicados por Internet, sin restricción por IP, se pueden dar diferentes casuísticas que degraden el servicio en diferentes puntos, llegando a la indisponibilidad.
  Estas casuísticas podrían ser:
  a. Saturación de la red por sucesivas llamadas malintencionadas. Esto significa que el equipo de un atacante realizará sucesivas llamadas a los servidores de nuestra empresa, con el objetivo de saturar los dispositivos de red por los que pase nuestro tráfico y dejar sin servicio

a esta, produciendo pérdidas económicas al no estar en funcionamiento hasta que se restablezca el servicio.

b. Existe una variante del caso anterior llamada DDOS, que en esencia se trata del mismo ataque pero en la hora de la verdad esa persona maliciosa tendrá más recursos a su disposición, normalmente una botnet. Una botnet es una gran cantidad de equipos o servidores normalmente conseguidos mediante la dark web, que se emplean para fines maliciosos, como en este caso, que el atacante podrá enviar llamadas multitudinarias a los dispositivos de red de la compañía desde múltiples orígenes, haciendo también más complicado su bloqueo.
c. Es posible que en épocas en las que se prevea una alta influencia de clientes, haya que reforzar la capacidad de red de la que se dispone, ya que si no, se podría estar sufriendo una denegación de servicio involuntaria al querer conectarse todos los clientes a la vez.

- Ataques de Nivel 7 (Aplicación). Asociados a malas configuraciones de los desarrollos, vulnerabilidades no consideradas o debilidades. Dentro de esta categoría entrarían los siguientes:
    - Cross site request (CSRF): el atacante es capaz de realizar una acción en nombre de la víctima, habiendo aprovechado previamente una inyección de código HTML en el servidor, la víctima establece una conexión legítima con el servidor que había sido vulnerado.
    - Inyección SQL: aprovechan vulnerabilidades de bases de datos para borrar datos, filtrar datos confidenciales, etc.

- Ataques asociados a backdoors. Ataques relacionados con mala praxis a la hora de activar/desactivar reglas de firewalls, activar o desactivar ajustes por defecto, etc.

- Ataques asociados a vulnerabilidades. Estos ataques pueden aprovechar vulnerabilidades existentes bien en los servidores o bien en los equipos de red, dichas vulnerabilidades pueden ser no conocidas.

- Ataques de Segundo nivel. Estos ataques están asociados a vulnerabilidades explotadas en ordenadores de usuario, de los cuales han conseguido tomar el control y que tratan de seguir avanzando a través de la infraestructura de red para tomar el control de los servidores.

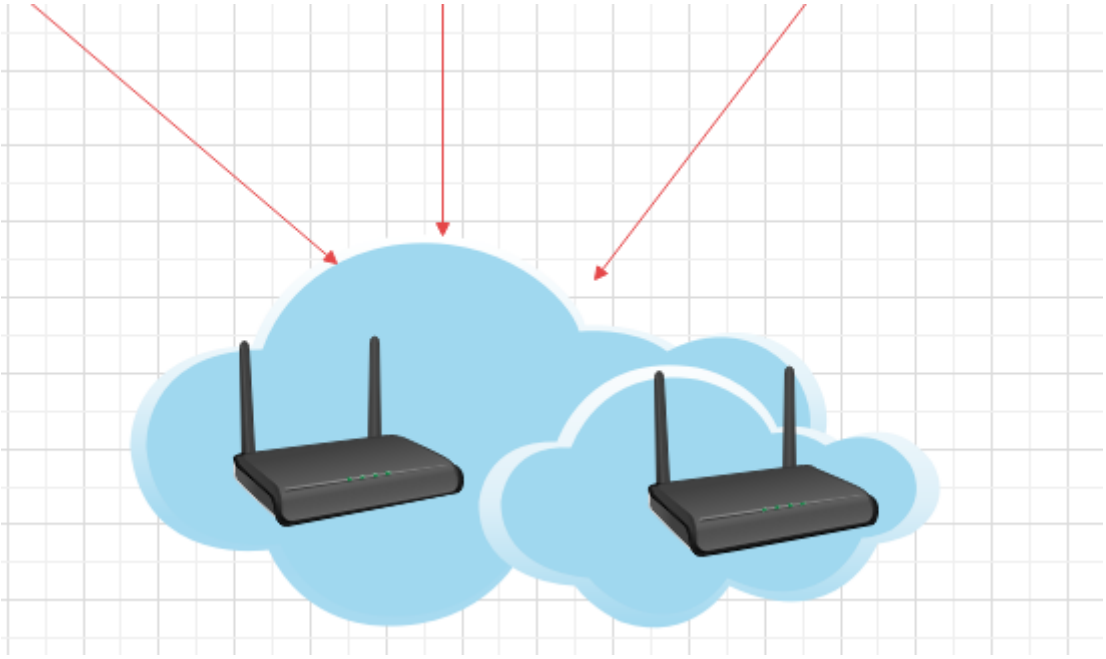
5.1 Denegación de Servicio (Nivel 3)

El ataque de denegación de servicio se produce por sucesivos intentos de apertura de conexiones con objeto de conseguir la degradación de la infraestructura tecnológica. Asumiendo la infraestructura desplegada el impacto puede estar

orientado a hacer un ataque por capas con diferentes niveles de penetración. Además, aunque se podría usar un servidor interno comprometido para atacar desde dentro la infraestructura, lo más probable es el ataque externo. **Este ataque externo solo se puede dirigir hacia las IPs públicas que forman parte del rango asignado para los servicios accesibles desde Internet**

Nivel I – Ataque de denegación de servicio al sistema de distribución del Datacenter

El sistema de distribución del datacenter, formado por uno o varios routers puede verse afectado por un ataque de denegación de servicio bien dirigido a nuestra empresa, bien dirigido a otro cliente de proveedor de servicio.



En ese caso el ataque se puede diseñar para:

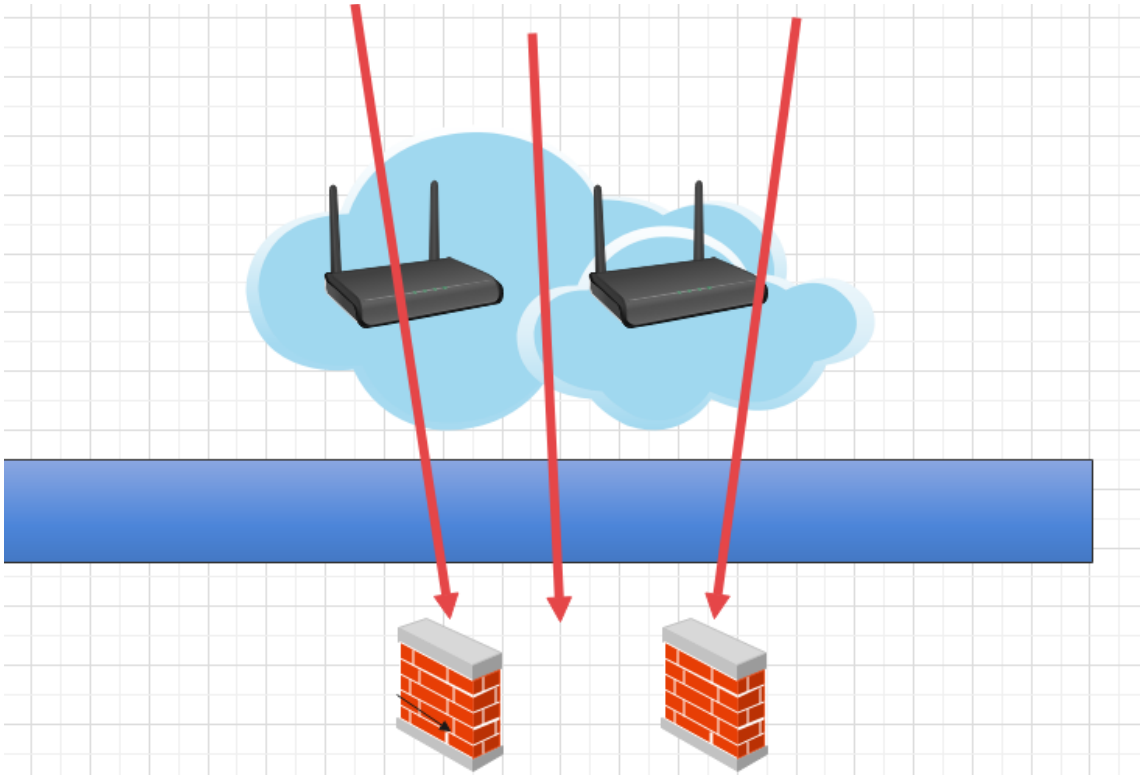
- Saturación por carga de tráfico, con el objeto de que se produzca descarte de paquetes en las interfaces de red. Se produciría una degradación del servicio, los routers empezarían a descartar paquetes de manera indiscriminada

- Saturación orientada al incremento de la memoria de los dispositivos de red. En este caso, el ataque está orientado a que se abran muchas conexiones, esas conexiones no se cierran adecuadamente, manteniendo las mismas tanto en la tabla de sesiones como en memoria del dispositivo. Llegado el momento, el dispositivo de red no puede seguir procesando tráfico y se origina degradación del servicio.

- Saturación orientada al incremento de la tabla de sesiones. El ataque está orientado a que se abran muchas conexiones “zombies”, es decir, que no se cierran adecuadamente, de esa manera se van acumulando sesiones de manera progresiva hasta que satura la tabla de sesiones y hay indisponibilidad total del servicio

Nivel II – Ataque de denegación de servicio a los firewalls perimetrales

Si el ataque añade un enmascaramiento adecuado, el mismo puede pasar del sistema de distribución a los firewalls perimetrales.



En este caso quedaría descartada la saturación de carga de tráfico en las interfaces de red y habría únicamente dos posibles causas:

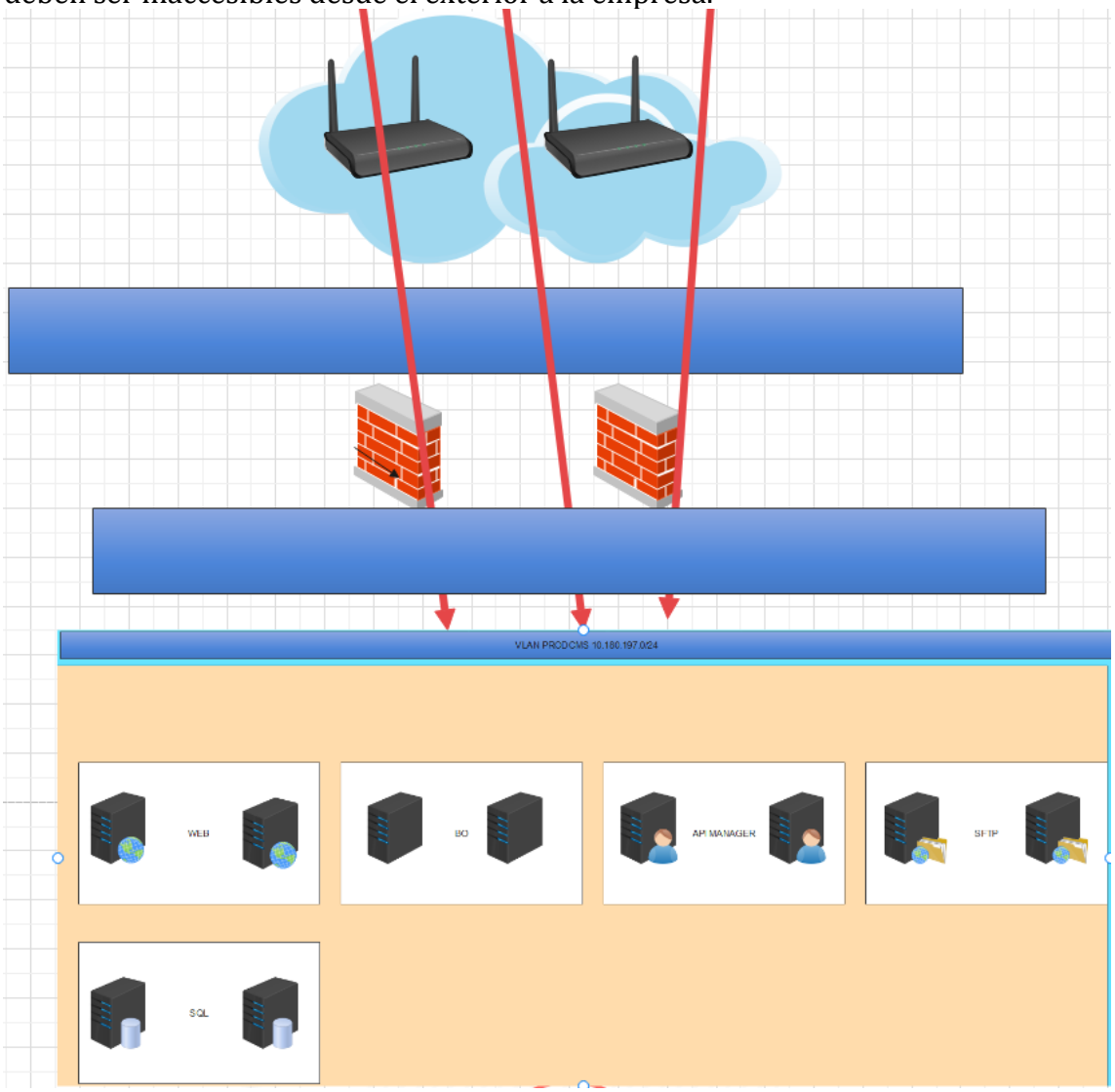
- Saturación orientada al incremento de la memoria de los firewalls. En este caso, el ataque está dirigido a hacer trabajar mucho la memoria de los firewalls, provocando una degradación del rendimiento hasta una caída efectiva de los mismos. En general, este caso es poco probable.

- Habitualmente, el ataque por denegación de servicio que más puede afectar a un clúster de firewalls es por saturación orientada al incremento de la tabla de sesiones (al igual que en un router). En general, una de las limitaciones más importantes de un clúster es la tabla de sesiones. Si se produce una apertura indiscriminada de sesiones que se mantienen vivas y no se cierran, la tabla de sesiones se va llenando, hasta que se satura y provoca el bloqueo del firewall y del servicio.

Nivel III – Ataque de denegación de servicio en los servidores

Si las conexiones se generan correctamente, siendo el ataque mucho más sofisticado, el ataque de denegación de servicio se produce contra el propio servidor, siendo un ataque en cascada.

Como anotación, y dado la estructura de la arquitectura de red, cabe anotar que los ataques se harán en los servidores publicados en las DMZ, ya que los de backend deben ser inaccesibles desde el exterior a la empresa.



En principio, la conexión https se termina en el balanceador. Desde el balanceador se abre una sesión segura a los servidores. En caso de una mala configuración del servicio, y ante un ataque, se lanzan muchas conexiones contra el servidor, el servidor las trata de procesar, sin embargo, progresivamente va aumentando el número de sesiones que trata de procesar manteniéndolas abiertas. Dado que van aumentando progresivamente el número de sesiones y las sesiones no se cierran, el servidor va aumentando el uso de la memoria y de la CPU hasta que termina de colapsar, tirando el servicio.

5.2 Ataques de Nivel 7 (Aplicación)

Estos ataques se generan con el objeto de aprovechar vulnerabilidades en la configuración de las aplicaciones/servicios web. Pueden tener diferentes objetivos como:

- Duplicado de la página web. Esto es muy común por ejemplo, a la hora de duplicar la web de una empresa como podría ser amazon, se utilizan gazapos de tipografía distintos de distinguir a simple vista, como usando de URL www.amaz0n.com , cambiando la o por un 0.
- Robo de credenciales
- Explotación de vulnerabilidades para hacer un ataque más profundo.

Las vulnerabilidades están siempre asociadas bien a una debilidad del producto/desarrollo, bien a malas configuraciones de ajustes. Estas debilidades pueden provocar que se produzcan inyecciones que permitan extraer datos o ejecutar scripts, pueden utilizar esta mala configuración como cabeza de puente para un ataque más elaborado (esa cabeza de puente permite, por ejemplo, ir escalando privilegios desde la aplicación hasta tomar el control de diferentes elementos de la red), pueden utilizar las vulnerabilidades para hacer redirecciones o pueden ser de tal magnitud que permitan extraer credenciales.
Al estar asociados con la capa de aplicación, el ataque está dirigido a aquellos activos que son accesibles bien directamente, bien indirectamente a través de Internet.

Ataque a URLs
Los ataques de nivel 7, habitualmente no son ataques de fuerza bruta, son ataques muy bien dirigidos que únicamente necesitan un par de conexiones a las URLs para poder acceder a los mismos. Hacen una explotación de una vulnerabilidad.
Desde el punto de vista de publicación de activos críticos, nuestra empresa presentará 3 posibles candidatos a realizar este tipo de ataques:

- Web Corporativa
- Punto de venta
- API

El resto de los elementos pueden ser usados como cabeza de puente, para realizar ataques más profundos.
En principio, el ataque iría sobre la VLAN DMZCMS tal y como se puede ver a continuación.

8. Escenario en detalle: Indisponibilidad lógica de Sistemas

8.1. Introducción al riesgo

El escenario de Indisponibilidad Lógica de Sistemas de Información (LUIS) está basado en la consideración de una situación en la que existen varios elementos de fallo/comprometidos dentro de la infraestructura lógica que hemos creado. El riesgo tecnológico, asociado a este escenario, considera una indisponibilidad lógica (encriptación de servidores, problemas con la integridad del dato, procesos extraños que impiden el correcto funcionamiento de los elementos de la infraestructura) de elementos críticos de la infraestructura que desembocan en la declaración de desastre, es decir, no se puede
operar y los tiempos de recuperación exceden de los que garantizan un mínimo impacto, tanto a nivel comercial, reputacional o de viabilidad de la compañía.
La activación de la respuesta al incidente relativa a la indisponibilidad lógica se puede basar en:

- La sospecha/certeza de que uno o varios servidores han sido comprometidos.
- La sospecha/certeza de que uno o varios servidores han sido afectados por un malware.
- La sospecha/certeza de que el AD ha sido comprometido.
- La sospecha/certeza de que la BBDD ha sido comprometida.
- Conexiones no habituales entre servidores que denotan un intento o incluso éxito en la pivotación entre los mismos.
- Aparición de procesos sospechosos/callbacks

Las suposiciones, anteriormente mencionadas, son algunos, no todos, disparadores de un plan de respuesta. Sin embargo, no todos los elementos de la infraestructura son críticos ni tampoco se puede hacer una recuperación simultánea de los elementos afectados, ya que, habría que establecer un orden de prioridad basado en el negocio.

8.2. Consideraciones previas a la recuperación

Para llevar a cabo una correcta recuperación de los sistemas, en un escenario de desastre asociado a la indisponibilidad lógica de los mismos, se hace necesario evaluar el peor caso, consistente en una modificación de la integridad de los datos (un tercero ha conseguido ganar acceso a los sistemas, generalmente al AD y puede tener el control parcial o total de los accesos a la plataforma) o bien se ha llevado a cabo la encriptación de los servidores
por una vulnerabilidad existente explotada mediante un malware.

Dado la falta de certeza sobre el alcance de la explotación, el timeline del ataque y la afectación o no de la integridad del dato, se hace necesario plantear
una estrategia que se base en dos niveles de actuación:

- Recuperación temprana de los sistemas de producción. En caso de un ciberataque a la plataforma es probable que el objetivo final sea la encriptación de toda la lógica de los sistemas de información, asumiendo la lógica como la encriptación de servidores, robots de backups, robots de almacenamiento, etc.

La duración media de la indisponibilidad en este tipo de ataque es de 3-5 semanas en función de la gravedad, elaboración y objetivo de los perpetradores del ataque. Es por ello, que el objetivo principal es conseguir acortar el tiempo de recuperación mediante el almacenamiento de copias maestras de todos aquellos sistemas que constituyen el core de negocio.

- Garantizar la integridad del dato. La clave de un ataque dirigido es la capacidad para realizar operaciones con los datos. Estas operaciones pueden estar orientadas al secuestro de los mismos (de tal manera que a la compañía le resulte imposible seguir operando y no le queda más remedio que pagar un rescate), a la modificación de la integridad del dato (mediante la modificación de los datos almacenados en las tablas de la base de datos), a la exfiltración de los mismos (mediante una extorsión a la compañía con objeto de que se pague un rescate para evitar la exfiltración) o a todas las casuísticas a la vez, en el peor de los casos.

8.3. Estrategia de recuperación

Tal y como se ha comentado en la sección anterior, la estrategia debe estar orientada a la rápida recuperación de los sistemas críticos, así como, a minimizar el proceso de recuperación de los datos tratando de que la conciliación manual sea reducida al máximo. La estrategia propuesta se basa en:

- Generación y custodia desatendida de una copia maestra de los sistemas críticos de producción mediante el clonado (snapshot) de los sistemas identificados como críticos
    - El objetivo de la copia desatendida es mitigar el riesgo asociado a la falta de integridad de los backups de los sistemas. La propuesta, que está orientada a la rápida recuperación, es realizar una copia maestra, dependiendo de la criticidad del servidor, cada 3/6 meses o cada año.
- Generación de una copia maestra del AD
    - Aunque un clonado del AD presenta ciertas dificultades técnicas a la hora de realizar la configuración de este, el grado de crecimiento de la compañía no requiere la exigencia de realizar continuas copias por lo que la copia maestra
- En cuanto a BD, dependiendo del enfoque de cada una de ellas y su función, la estrategia es distinta:
    - Si tenemos una BD que sirve de apoyo para aplicaciones, se puede realizar una copia maestra anual, asumiendo que los datos almacenados pueden ser recuperables, si no se hará cuando se considere conveniente
    - En el caso de una base de datos que almacene copia de los datos de clientes, se hará de manera anual.

8.4. Respuesta al incidente

La detección de un comportamiento anómalo debe conducir al aislamiento de la plataforma y su posterior recuperación. Tras la detección de un malware, proceso no identificado o sospechoso de ser malicioso, se debe proceder al aislamiento de la plataforma a nivel de VLAN, así como el desacople de las VLANes pertenecientes a las workstations (Headquarters de aquí en adelante, HQ) de usuarios con el Datacenter.

- Desacople de HQ

En el caso de un problema de seguridad en los servidores es necesario proceder al desacople en los firewalls que lo conectan con el datacenter.
Para ello se creará la siguiente regla:

Direcciones de origen	**Direcciones Destino**	**Puerto**	**Acción**
IPs HQ	IPs Datacenter	Todos	Deny

De esta forma, independizamos ambos entornos y evitamos la propagación de malware entre ellos.

- Desacople publicación Servicios

Si se confirma la aparición de un ransomware por ejemplo en la plataforma de servidores, con una encriptación progresiva de los mismos, es necesario cerrar las conexiones que pueden realizar un posible callback hacia Internet para confirmar la encriptación. En ese caso en el FW es necesario poner la siguiente regla, sobre todas las demás. Con esta denegación cortamos callbacks y propagación del malware.

Direcciones de origen	**Direcciones Destino**	**Puerto**	**Acción**
IPs Servidores	Any	Todos	Deny

- Con objeto de ir preparando la recuperación de los servidores, es necesario aislar las redes. En el caso de un ransomware que proceda al contagio progresivo de todos los equipos que están conectados en una misma VLAN y con objeto de aprovechar la ventaja de la segmentación de red, es necesario aislar cada VLAN dedicada a servidores con el resto de ellas
- El siguiente paso es evitar la propagación lateral dentro de una misma VLAN. En este caso, es necesario deshabilitar las tarjetas de red de los servidores y cada una de las VLANes, de esta manera se garantiza que no existe ningún tipo de propagación.
- También sería necesario deshabilitar las backups, ya que si se realizan sobre sistemas ya encriptados podríamos comprometer la integridad de los datos de servidores críticos

Vamos a imaginar dos escenarios distintos, uno en el que se encuentran comprometidos un número reducido de servidores y un segundo en el que toda la planta está comprometida.

Escenario 1: Número limitado de servidores

En este caso, la prioridad es restaurar la plataforma **excepto el servidor contagiado**.

Sería necesario una identificación de dicho servidor para revisar el proceso corriendo que ha generado la encriptación del mismo. Esta comprobación se debe realizar con las redes aisladas y con la tarjeta de red deshabilitada.

1. Dentro del segmento de red a levantar, es necesario revisar individualmente cada servidor para comprobar que no se han contagiado, comprobando los procesos que corren en ellos y haciendo una comparación con los procesos del servidor afectado.
2. Una vez hecho esto, se van levantando los servidores del segmento de red aislado. Una vez se han levantado de nuevo, sin posibilidad de comunicación entre ellos, se vuelve a habilitar la tarjeta de red.
3. Se debería observar la plataforma durante un tiempo como precaución, con objeto de revisar a nivel de logs, posibles callbacks o ejecución de procesos en servidores
4. Si no se encuentran indicios de actividad sospechosa, se deshabilitan las reglas de FW creadas anteriormente para establecer de nuevo la comunicación entre VLANes y HQ.
5. Si el servidor contagiado es considerado crítico, restauraremos el backup más reciente, comprobando su integridad mediante un hash por ejemplo previamente.

Escenario 2: Compromiso total de la plataforma

En este caso lo primero es identificar el servidor contagiado para identificar el proceso que lo originó, tal y como antes con las tarjetas de red deshabilitadas y las redes aisladas. A partir de aquí procedemos a restaurar:

1. Directorio activo: Para realizar esta recuperación es necesario que no haya ningún servidor conectado de manera lógica a su VLAN. En este punto seguramente no se conozca el estado global de la plataforma, por lo que para asegurar la producción se recuperará una copia de seguridad e instalarlo en su VLAN.
2. Recuperación del DNS: misma estrategia que con el caso anterior
3. Recuperación de los entornos de Preproducción: es necesario que la regla que se aplicó como precaución para aislar los entornos no afecte a estos subrangos de red a partir de ahora para su correcta recuperación
4. Levantar servidores del backend de Producción: dado que este entorno es crítico en sí, hay que seguir el siguiente orden:
    a. Cargar el backup
    b. Comprobar los procesos sospechosos en este
    c. Comprobar que no hay intentos de conexiones con el exterior

    Este proceso se debería realizar de manera recursiva para todos los servidores que forman parte de este entorno. Una vez hecho esto, se procederá a la restauración de las bases de datos de producción.
    Por último, volvemos a habilitar sus tarjetas de red y conexiones normales.
5. Resto de entornos: esto se realizará evitando que el servidor infectado vuelva a infectar la plataforma de nuevo.