GUIDANCE

Secure design principles

Guides for the design of cyber secure systems

PAGES

Pages

PUBLISHED

21 May 2019

REVIEWED

21 May 2019

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations

Public sector

Cyber security professionals

Large organisations

Getting the most from the secure design principles

These principles are intended to help ensure that the networks and technologies which underpin modern life are designed and built securely.

The problem

To be useful, systems very often need to move, store and provide access to sensitive data. Unfortunately, this makes them prime targets for cyber attack. If these systems are successfully compromised, the fallout can be damaging, expensive and embarrassing.

However, the picture need not be a bleak one. Frequently, the very worst outcomes can be avoided if services are designed and operated with security as a core consideration.

With this in mind we have developed a set of principles to guide you in the creation of systems which are resilient to attack, but also easier to manage and update.

System design

Throughout this guidance, we use the term **system**, by which we mean 'a collection of digital components that are connected using communication technologies to perform a business function.' A good example of the sort of system we are describing here is the UK's online passport application service, but it could refer to many other digitally-enabled business functions.

We will also use the term **cyber-physical system**, by which we mean 'a system that measures or controls the physical world to achieve a particular goal.' A good example is a modern car, in which complex logic measures the physical environment in order to control the movement of the vehicle.

The principles have been conceived to be applicable to both digital systems and cyber-physical systems.

Audience

This guidance is aimed at people who design systems. The principles are most useful in the design and build phases of a project, although they can also be used to review existing systems.

How this guidance is structured

Applying the principles will require some customisation to suit your particular situation. For example, the exact requirements of an online information service will be different to the remote management of a power station. However, the principles will guide your considerations in either case.

The Cyber Security Principles offer the most generally applicable advice. The Virtualisation Design Principles apply to the more specific case of systems which rely on virtualisation technologies.

We have divided each set of principles into five categories, loosely aligned with stages at which an attack can be mitigated:

- **Establish the context**
  Determine *all* the elements which compose your system, so your defensive measures will have no blind spots.
- **Making compromise difficult**
  An attacker can only target the parts of a system they can reach. Make your system as difficult to penetrate as possible
- **Making disruption difficult**
  Design a system that is resilient to denial of service attacks and usage spikes
- **Making compromise detection easier**
  Design your system so you can spot suspicious activity as it happens and take necessary action

- **Reducing the impact of compromise**
  If an attacker succeeds in gaining a foothold, they will then move to exploit your system. Make this as difficult as possible

Cyber security design principles →

Topics

Critical National Infrastructure (CNI)

Security architecture

PUBLISHED

21 May 2019

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations

Public sector

Cyber security professionals

Large organisations

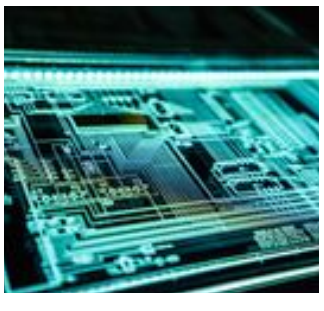
Was this article helpful?

Yes No

Also see

New SOC guidance 101
Explaining the rationale behind the NCSC's updated Security...

Blog Post
23 May 2022



Building a Security Operations Centre (SOC)
Guidance to help organisations design a SOC and security...

Guidance

The Technology Assurance principles

Covering the ‘Product development', 'Design and...

Blog Post
11 May 2022