A Spotlight On...

IT Asset Management

Background

As the business use of technology grows rapidly, it is difficult to understand what is being used, by whom, and for what purpose.

Your security is only as strong as your weakest link. If you are not tracking technology in the form of business applications or infrastructure it could mean a bad day at the office.

Particularly for larger, more complicated organisations where change has been a constant, establishing effective IT asset management can be a very difficult endeavour.

Why is IT asset management important for security?

Effective security relies on an accurate, up-to-date inventory of IT assets. This on its own, however, is not sufficient. You also need to understand the level of potential information risk associated with each asset. These risk levels should steer security investment planning and inform the prioritisation of related security activity.

Configuration management databases (CMDBs) and other lists of servers and applications might feel like 'job done', but such data can readily go out of date, contain significant gaps, and only provide superficial information.

Our five key steps will bring significant benefits — but it is not easy

1. **Mapping devices to apps and services** – understand device connections, dependencies, and business criticality.
2. **Automated device discovery** – all live devices are in a CMDB and decommissioned devices identified.
3. **Up-to-date software inventories** – all unpatched and unsupported software instances are detected.
4. **Asset business criticality impact scores** – enables risk prioritisation of security control rollouts and remediation.
5. **Asset hygiene** – completed critical fields, e.g. Owners, Hostnames, IP Addresses, Device Type, Asset Criticality.

These activities provide an organisation with the confidence that:

- All IT assets have been identified and security control coverage is understood.
- Security, technology, and business teams can prioritise security remediation activity based on the criticality of the business services that the IT assets support.
- A foundation exists for better visibility across multiple security domains, e.g. vulnerability, access, and incident.
- Cyber security control gaps are better prioritised.
- Change management is less risky due to improved inventories.

How i-confidential can help

We have assisted a number of clients with their IT asset challenges, and developed our experience and 'know how' in this area. This enables us to offer a structured programme of activity:

- Establishment of key principles and desired outcomes for the IT asset management improvements needed to support effective cyber security.
- An implementation approach that includes requirements for improved IT asset management systems, discovery processes, and operating models.
- Support for closing gaps against the above requirements utilising our proven **Security Remediation** approach.

For more information about how we can help your business, please contact us

i-confidential
Building Trust, Reducing Risk

www.i-confidential.com
info@i-confidential.com
0131 445 1458