ARCULUS CYBER SECURITY

Newsletter

Welcome to our latest newsletter, and what an exciting time it's been! In April, we celebrated our first birthday with a whole company get-together in the Shard in London. It was great to see everyone in person, after all the months of remote working and Teams calls. We enjoyed presentations on a number of interesting topics, including Zero Trust (see article below).

Our team and project portfolio continues to grow, and here are just a few highlights:

CREST Accreditation of Arculus for Vulnerability Assessment

Adding to our previous CREST certification for Penetration Testing, Arculus is now CREST-accredited for Vulnerability Assessments. A security vulnerability is an unintended defect that leaves organisations vulnerable to attack. If unpatched, software and hardware will contain numerous vulnerabilities, and these are used by attackers to gain a foothold to launch potentially serious attacks. Vulnerability Assessment can find these before the attackers do, and allow you to patch.

Arculus uses leading industry tools to support our CREST Vulnerability Management Platform. We offer a range of options, including monthly external and internal scanning, configuring scans for in-house staff to run, and review of report findings to highlight any significant issues. This can help you to proactively reduce your cybersecurity risk cost-effectively.

CREST

VA PEN TEST

Arculus exhibits at CyberUK 2022

In May, we were very excited to be able to exhibit at the NCSC flagship event, CyberUK, held in Newport this year. We were delighted to see so many people visiting our stand and catch up with friends and clients old and new.

New Cyber Essentials / Cyber Essentials Plus requirements

Since January 2022, Arculus consultants have been helping many customers to meet the new requirements of IASME Cyber Essentials / Cyber Essentials Plus. The new version must be used for all new and renewal certifications, and the following are the main changes:

- Added a home working requirement and information on how this is to be included in the scope of certifications.
- All cloud services are now in scope, added definitions and a shared responsibility table to assist with this.
- Extended the multi-factor authentication requirement in relation to cloud services.
- Updated the password-based authentication requirement and added a new section on multi-factor authentication.
- Thin clients are now in scope and added to the 'devices' definition.
- Added a new device unlocking requirement to the 'secure configuration' control.

These changes have brought more into line with current ways of working, but it does mean some new tests are required. Arculus can help you meet the new requirements by providing consultancy, such as pre-certification audit and gap analysis.

IASME CONSORTIUM

Zero Trust Architecture

We've heard a lot about Zero Trust Architecture (ZTA), including this statement from National Security Agency (NSA):
"As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services."
Many vendors are producing solutions to support a ZTA, but there are challenges, including:

- Maturity of vendor products to support a ZTA.
- Organization's ability/willingness to migrate to a ZTA because of:
    - o heavy investment in other (legacy) technologies
    - o absence of, or deficiency in, identity governance
- lack of ability/resources to develop a transition plan, pilot, or proof of concept
- Interoperability concerns for ZTA products/solutions with legacy technologies such as:
    - o standard versus proprietary interfaces
    - o ability to interact with enterprise and cloud services

Arculus Security Architects can help you design and implement solutions to follow ZTA principles effectively, and make best use of your investment in tools and technologies.

ISO/IEC 27001 and 27002 are changing!

The new version of ISO/IEC 27002 (the code of practice) was published in February, with ISO/IEC 27001 (the standard) due to follow in the autumn. This is the first update since 2013, and brings a number of key changes:

There are now 93 controls rather than the previous 114.

These controls are grouped into 4 'themes' rather than 14 clauses:

- People (8 controls)
- Organizational (37 controls)
- Technological (34 controls)
- Physical (14 controls)

Continued on the next page...

There are 11 brand new controls:

- Threat intelligence
- Information security for use of cloud services
- ICT readiness for business continuity
- Physical security monitoring
- Configuration management
- Information deletion
- Data masking
- Data leakage prevention
- Monitoring activities
- Web filtering
- Secure coding

The controls are assigned five types of 'attribute':

- Control type (preventive, detective, corrective)
- Information security properties (confidentiality, integrity, availability)
- Cybersecurity concepts (identify, protect, detect, respond, recover)
- Operational capabilities (governance, asset management, etc.)
- Security domains (governance and ecosystem, protection, defence, resilience)

Organisations will have a transition period (usually 2 years) to migrate to the new version, but it is advisable to start planning this early. Arculus is already working with a number of customers to support them in migrating, and can provide you with advice and consultancy to ease the transition.

Cybersecurity in the news

The following are some articles of current relevance:

- The Verizon data breach report 2022 has been published. It is very interesting to see that Credentials and Phishing lie behind a large majority of data breaches. The full report may be downloaded here (registration required).

- NCSC has released new guidance on incident response, with a focus on staff welfare.

- NCSC has also published its 5th report on its Active Cyber Defence (ACD) programme. The top 5 take-downs in 2021 were:
    - o Extortion Mail Server
    - o Celeb Endorsed Investment Scams
    - o Fake Shop
    - o Phishing URL
    - o Web Shell

- With the final Microsoft 'Patch Tuesday' having taken place on Tues 14th June, who will miss it? The launch of their new Autopatch solution is intended to make life easier for sys admins and end users. We'll be interested to see if there is reduction in vulnerabilities due to unpatched devices.

If you would like to discuss anything in this newsletter or just chat to us, please contact: info@arculus-cyber.co.uk or call us on +44(0)845 299 3009.

ARCULUS CYBER SECURITY