ARMD digital™
advance risk mitigation digital

Protect Your Business and Your Customers: The Importance of Conducting Vulnerability Scans for Financial Service Providers

In order to deal with the current state of cybercrime, we need to shift our focus to include **proactive risk mitigation** as a way to reduce the likelihood of an incident occurring in the first place.

A vulnerability scan is one of the most powerful tools you can deploy to help you proactively defend against cyber threats.

Fight Fire With Fire

Because cyber criminals use these same tools to quickly assess the easiest entry-points to breach a company, vulnerability scanning can be seen as a pre-emptive first line of defence against cyber threats.

CyberProfiler Scan is a vulnerability scan which provides an Attacker's Eye View™ of a domain's (website) cyber risks.

The report alerts you to key information that criminals use to profile businesses in preparation for cyber attacks.

Viewing your exposure from an Attackers Eye View™ will help you optimise your online presence, reduce or change public information where possible, and ultimately limit opportunities available for attackers to defraud you.

Why are FSPs a Valuable Target for Cyber Criminals?

FSPs are at greater risk for cyber-attacks because they handle sensitive financial and personal information, making them a valuable target for cybercriminals.

Additionally, FSPs often have complex IT systems and networks, which can make them more vulnerable to security breaches.

Furthermore, FSPs are heavily regulated and a data breach can result in significant fines and reputational damage, meaning they may be more willing to succumb to Ransomware extortion.

With the increase of remote work, many FSPs face an even greater risk as the use of unsecured personal devices and home networks can create new vulnerabilities and potential entry points for cybercriminals.

What Does Our CyberProfiler Scan Report Provide?

- Provides businesses with a rapid snapshot of their digital estate from an attacker's perspective with **Findings**, **Observations**, and **Insights**.
- Highlights exposed systems that criminals leverage to deploy malicious software such as Ransomware.
- Actively scans for vulnerable technologies and configurations which malicious actors use to defraud a business, their customers, suppliers, or other third parties.
- Provides remediation recommendations, arming organisations with the knowledge to mitigate exploitable vulnerabilities.
- Analysis is driven by advanced intelligence tools that are continuously updated to include the latest cyber risks.

What Sort Of Risks Might My Report Reveal?

- Why you might be vulnerable to phishing attacks that target customers by spoofing your domain
- Where you might have insecure protocols with data being shared in plaintext
- How malicious emails could be sent from your domain
- Why you might be more prone to attacks or ransonware threats because of clear access point to attackers
- Where you are revealing too much information that can be spoofed by hackers
- Lists of expired certificates which present a danger
- Associated domains which may leave you vulnerable and provide easy targets for attackers
- Domain variants that attackers might register to appear legitimate when impersonating your company in phishing scams
- Lists of associated domains and subdomains for review so as to remove unused, reducing your online attack surface and helping to prevent malicious activity

Vulnerability Scans - Getting A Second Opinion

Some FSPs are unfortunately not unaware of vulnerability scans and the advantages of utilising them.

Many FSPs who are aware of vulnerability scans employ multiple vulnerability scanners to ensure complete coverage of all their digital assets, resulting in a complete picture.

If you're already using a vulnerability scanning service, getting a second opinion from a credible source can be very valuable – it will either provide peace of mind, or could alert to risks that weren't picked up.

When To Do A Vulnerability Scan

If you've never had a vulnerability assessment, then **the time is now**.

Each organisation will have its own risk management and compliance requirements, but we'd recommend running a scan at least **once or twice a year**.

Over and above this, you should run a scan **after any major system, organisation, or infrastructure change** (network changes, new system configurations, new user groups)

What Should I Do Once I Get My Report?

The report should be analysed in conjunction with the organisation's management and inhouse IT team or their outsourced IT MSP (Managed Service Provider).

The potential risks and vulnerabilities can then be quickly assessed and prioritised by separating them into **major risks** (that must be managed immediately) and **minor risks** (that may be acceptable).

What Does It Cost?

R1,500 (Incl. VAT) for first-time scans and R750 for all subsequent scans.

How Do I Order A CyberProfiler Scan And Get My Report?

We've made getting your CyberProfiler Scan easy and convenient, you can order and pay online.

CLICK HERE

Regulatory Environment

In the **Regulatory** section on our website, we provide a list of laws that are relevant to our products and services, giving a concise overview of each section that we've identified as relevant. The laws we've identified demonstrate how our products and services can help you to comply with the legal and compliance obligations set out in the law.

Regulations include: Financial Advisory and Intermediary Services Act (FAIS), Protection of Personal Information Act (POPIA), Joint Standard | Cybersecurity and Cyber Resilience Requirements for Financial Institutions, Joint Standard | Information Technology Risk Management for Financial Institutions, King IV Report and King Code, Cybercrimes Act.

CLICK HERE

About Us

ARMD.digital is based in Cape Town, South Africa and was formed as a division of Genlib in August 2022. Genlib is an authorised FSP (Financial Services Provider) providing innovative insurance solutions to Brokers and their clients in South Africa since 2008.

Simplify identification of cyber security risks

We want to make it as simple as possible for businesses to identify cyber security risks. For this reason, we partnered with **STORM Guidance**, a London-based specialist cyber risk and cyber incident advisory firm, in order to make their service accessible through an online portal - **www.armd.digital**

STORM's specialists have decades of experience in helping clients recover from a range of cyber incidents, including Ransomware, Business Email Compromise (BEC), Extortion and Data Theft.

STORM has helped some of the world's leading underwriters and their customers with risk management.

Founder, Neil Hare-Brown, has been working in cybercrime for over 3 decades. He helped form the first digital forensics lab with the MET police in the mid-90s and written a book "Information Security and Incident Management" in association with the British Standards Institute.

ISO 27001:2017 certified | ISO 9001:2015 certified | ISO 14001:2015 certified

Certified for the following activities: Risk and security consultancy providing services encompassing cyber incident response, assessment, planning and training to commercial customers across the UK and internationally.

In November 2021, STORM partnered with QBE European Operations to roll out its CyberProfiler tool.

QBE Insurance Group is one of the world's top insurers and reinsurers, providing cover in more than 140 countries.