Welcome to KYND

Cyber risk management experts KYND proactively help your clients understand their organisation's exposure and protect against the ever-growing cyber threat landscape with the help of the KYND Signals Report.

This guide explains some of the KYND key red and amber risk indicators as your clients use the report to understand and mitigate the cyber vulnerabilities posing a risk to their organisation.

How does KYND find these vulnerabilities?

KYND non-invasively scans for publicly visible software and services that are owned by an organisation and visible on the Internet. We don't scan IP ranges, instead using the the information in the global WHOIS data to locate potential vulnerabilities sharing the organisation's domain(s)'s registrant information.

What is being looked for?

KYND is looking for any instances of exposed services or critical software vulnerabilities that would significantly increase an organisation's exposure to cyber-attacks. This helps the underwriter assess the cyber risk posture, and determine if there is a need to take any actions prior to agreeing on a policy.

Key indicators explained

Essential actions

RDP

Remote Desktop Protocol (RDP) is a system developed by Microsoft that provides a user with a graphical interface to connect to another computer over a network connection. Having a DP service directly visible and accessible from the Internet can make an organisation extremely vulnerable to cyber-attacks.

VNC

Virtual Network Computing (VNC) is a system that enables a user to remotely control another computer. Having a VNC service directly visible and accessible from the Internet can make an organisation critically vulnerable to cyber-attacks.

KEY INDICATORS

RPC

A remote procedure call (RPC) is when a computer program causes a program to execute on another computer. Having certain RPC services directly visible and accessible from the Internet makes an organisation highly susceptible to cyber-attacks.

Samba

Samba or Server Message Block (SMB) is a communication method providing shared access to files on a network. In certain circumstances, having Samba services directly visible and accessible from the Internet puts an organisation at risk of cyber-attacks.

Missing/invalid SPF on Primary Domain

SPF stands for 'Sender Policy Framework', and it's an email authentication technique that is used against email spoofing. An SPF record allows a domain owner to publish a list of the domains or IP addresses that should be trusted to send emails for a given domain. Not having SPF properly configured for a domain means that anyone can send an email pretending to be from that domain.

Missing/invalid DMARC on Primary Domain

DMARC stands for 'Domain-based Message Authentication, Reporting and Conformance'. It's an email validation system designed to protect a company's email domain from being used for email spoofing, phishing scams, and other cyber crimes. Without a DMARC policy in place, emails impersonating an organisation can bypass security measures and be delivered to recipient inboxes.

Advisable actions

Windows Powershell

Windows PowerShell is an automation, administration and management tool developed by Microsoft. It can offer very highly privileged access to certain systems. Having Windows Powershell services directly visible and accessible from the Internet can make an organisation deeply exposed to cyber-attacks.

TeamViewer

TeamViewer is a proprietary software application that supports the remote control of computers. Having Team-Viewer services directly visible and accessible from the Internet can make an organisation vulnerable to cyber-attacks.

Out-of-Date or Vulnerable Developer Access Services

Developer access services enable a direct connection to the computer systems running your business. Running any software that is out of date or with a known vulnerability makes this service susceptible to attack and service failure. Newly discovered software vulnerabilities are disclosed publicly to warn all users of the vulnerable products and as part of the resolution process for software developers. Unfortunately, attackers also share tools and techniques that can be used to exploit these weaknesses as soon as they are publicly disclosed.

End-of-Life Microsoft Software

Windows Server 2008 reached 'end of life' on January 14th 2020. This means it is no longer supported by the manufacturer and any new security vulnerabilities discovered will no longer be fixed and can be specifically targeted and exploited by hackers. With no product support, continuing to run this server after this date makes an organisation exposed to attack and service failure.

Here to help

If you have any questions about KYND, its services or technology, get in touch with our experts at signals@kynd.io.

Exposed Databases

A database should not be using a port that is directly visible and accessible from the Internet. Open access allows attackers to easily launch their attacks to gain entry into this system, allowing them to control assets, exfiltrate data or install ransomware. This could result in a breach of sensitive information.