Texas Council Risk Management Fund

KYND Scans

Staying on top of Cyber Security threats is a team effort. Dedicated IT staff, management, and regular employees all play a part in a quality Cyber Security management framework. However, a little extra help to identify threats and gaps in security policies can take some of the stress away from staff. In August, the TCRMF Board contracted with KYND to assist members with vulnerability scans. Here is information on what KYND is providing to members.

KYND performs external and non-invasive scan of TCRMF member domains quarterly. KYND will only see what is externally visible on the internet. The scans won't identify anything 'behind the curtain' or member's firewall perimeter. KYND will see open ports and services running on them, but they may not be able to tell whether these directly connect to a member's database/-network/back-end. KYND can identify certain information about vulnerabilities such as Fully Qualified Domain Name, registrant email and organization, IP, Port, Internet Service Provider, services, and product version. KYND does not store MAC addresses, Secure Socket Shell host keys, and other unique identifiers. Here are some risks that can be identified with KYND scans:

Email Risks
Any organization that has not put the standard email protections in place is immediately at high risk of having these addresses spoofed or impersonated to defraud its employees, customers, partners, and suppliers. Email impersonation fraud, otherwise known as Spoofing, Business Email Compromise, or CEO fraud, is the most frequently reported cyber fraud loss. To protect against these risks, there are standard protections available which should be implemented by every organization to reduce this threat.

Known Vulnerabilities
This risk relates to services that have been identified which contain a known vulnerability to attack or compromise. Newly discovered software vulnerabilities are disclosed publicly to warn all users of the vulnerable products and versions 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 or even before they are publicly disclosed. Search engines are then used to easily identify and target services which are known to have a specific vulnerability. All the above can happen within days or even hours of a new vulnerability being disclosed.

Running services which are known to be vulnerable carries a real risk of the following:
• Theft of data. Hackers can easily exploit vulnerabilities to directly access sensitive data.
• Loss of control of website. Website owner and visitors can be unaware that the site and traffic to the site has been compromised.
• Ransomware, a malicious program that removes access to electronic files, usually by Encryption.

• Malware, software specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Misconfigured Services
Some services should never be directly accessible from the Internet. Examples of such services include:
• Databases which may contain personal or sensitive commercial data.
• Developer or administration access points to computers.
• Routers or network equipment.

These types of services will immediately attract the attention of attackers and should be hidden behind firewalls, strongly enforced logins or only be accessible via a VPN. There are regular incidents reported of organizations leaving databases containing sensitive data freely accessible directly from the Internet.

Phishing and Malware Risks
Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details for malicious reasons, Malware is malicious software designed to infect the computer of any visitor to that page, with the intention of gaining control of the computer, stealing data, or even holding that data to ransom (also known as ransomware).

If an organization's websites are being used to host phishing and/or malware attacks they will be immediately blocked by all the major browsers and their customers will not be able to reach them. Visitors to their site will also be exposed to the threats mentioned above. This represents a significant risk to business continuity and reputation.

The TCRMF Cyber Risk Services Advisor is ready to schedule Cyber Risk Assessments and Incident Response Plan Tabletop Testing visits for members. To get on the schedule, contact Lee Cain, Cyber Risk Services Advisor by email Lee.Cain@sedgwick.com or by phone 512-619-1437.