Cyber Risk Exposure Report

Apr 2022

Executive Summary

Target >> eXample™

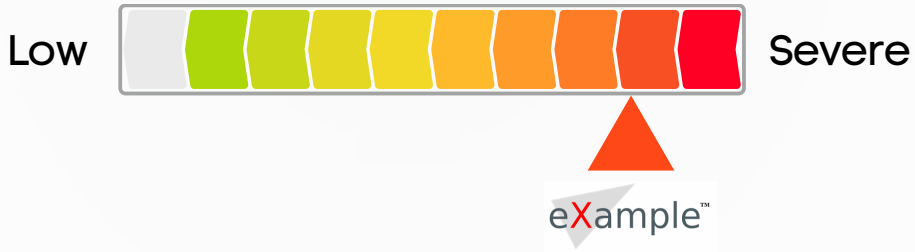
Overview

This report is intended to provide a high level 'Red Flags' report to the target organisation on their current Visible Cyber Risk Exposure.

The report provides insight into several key areas of Cyber Risk so that the target organisation can better understand their current exposure, their 'Attack Surface' and serve as the basis for further actions.

To compile this Report, investigations and reconnaissance have been carried out to ascertain the current state of Visible Cyber Risk and determine a current 'Attacker View' of the Target organisation.

Example - Current Cyber Risk Exposure



Ransomware

Exposure has been identified

Open Access

Exposure has been identified

Dark Web

Exposure has been identified

Cyber Risk Exposure

Target >> eXample™

Ransomware

Database exposed & directly visible

Example Co - A MySQL database is currently using port 33xx on IP address 195.224.xx.xxx This is an open port which is directly visible and accessible from the Internet.
At worst this may expose sensitive information directly to the internet, at best it elevate the risk of sustained efforts to compromise your systems, and we recommend this is urgently addressed.

- Ransomware
- Malware
- Public/unsecured assets
- Control of assets

Open Access

Remote Desktop Protocol **visible and accessible from the Internet.**

When remote desktop services are visible to the internet, hackers are able to identify services with vulnerabilities which they will then exploit. Having a visible remote desktop makes an organisation **extremely vulnerable** to cyber attack and service failure, we recommend this is urgently addressed.

- Public/unsecured assets
- Control of assets
- Ransomware
- Security

Dark Web

Dark Web Breach Exposure
This report identifies breached credentials from users with email addresses under the mail domain "@exampleco.com".

These credentials are obtained from websites, databases and various online services that have been breached, likely due to either a technical vulnerability or social engineering attack.

Compromised Accounts	3,413
Passwords Leaked	3,128
Data Items Leaked	915

Cyber Risk Exposure

Target >> eXample™

What to do next - Top 3 Issues to Address

1

Close Public Access to Database Services

Why is this important?

There are 1x SQL Databases open to the public, allowing others to control assets or install malware / ransomware. Even if these databases are protected by passwords, open access allows attackers to easily launch their attacks and gain entry into these systems.

Databases should be protected behind firewalls and access restricted to internal networks to prevent attackers gaining access to Example Co's internal and customer data.

2

Close RDP Access to your Infrastructure

Why is this important?

There are 2x Remote Desktop Protocol (RDP) services open to the public. RDP is commonly exploited to deploy ransomware and steal data, making Example Co extremely vulnerable to these types of attacks. RDP services should be protected behind firewalls and restricted to internal networks.

Additionally, RDP access should only be granted to Example Co systems and accounts where absolutely necessary, and multi-factor authentication (MFA) should be required in these limited cases.

3

Implement Email Policies

Why is this important?

@exampleco.com does not have a DMARC policy to prevent spoofed emails from being delivered that appear to be legitimately sent from your business. Even if you have inbound mail protection solutions, these will not prevent criminals from sending spoofed outbound emails to your clients, suppliers and other vital business contacts.

This puts Example Co at significant risk of Financial Loss due to Business Email Compromise, which can lead to issues like payment of fraudulent invoices or unauthorised payments being made which you could be liable for.