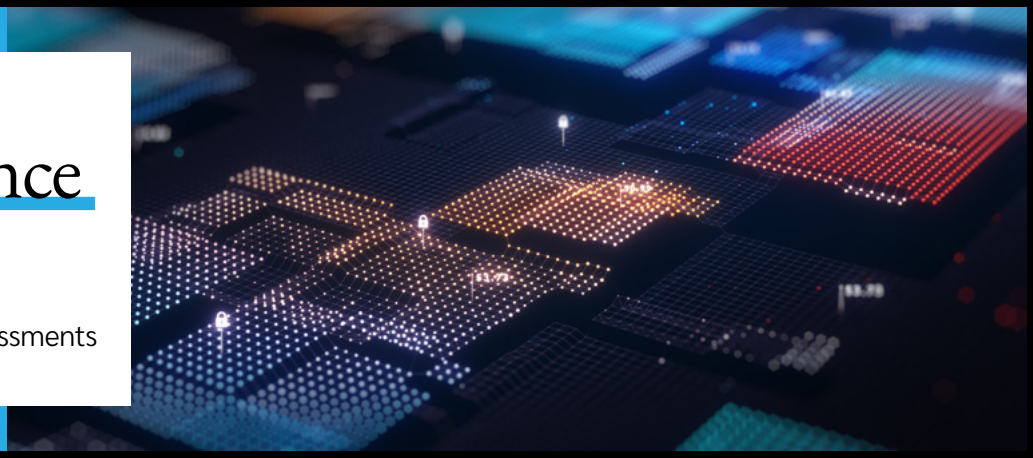
Cyber Insurance Explained

Open Port and Vulnerability Assessments



Taking Action to Protect Your Business from Cybercrime

Over the past few years, insurers have taken a proactive approach to preventing cybercrime, conducting automated network footprinting, at policy renewal and/or throughout the policy period. Doing this allows insurers to simplify the insurance application process, and to detect vulnerabilities and potential compromises.

The mutual aim is to prevent an attack on your business.

Insurers undertake these external scans by utilising:

1. the primary domain name of your organisation;

2. the WHOIS database;

3. certificate data; and

4. passive Domain Name System (DNS) records,

to analyse hundreds of data points about your business. Amongst other vital pieces of information, the analysis highlights third party dependencies and open Remote Desktop Protocol (RDP) ports.

Detecting Vulnerabilities with Non-Intrusive Scans

Insurers may also utilise mid-policy scans, to look for any interim changes. For example, identifying RDP or SMB ports that might be exposed to the internet, or new vulnerabilities that are added to the Common Vulnerabilities and Exposures (CVE) list (and therefore often exploited by cyber hackers).

Insurers may have different approaches but are primarily concerned about ports or services that may permit remote access into your network. These may include, for example:

1. VNC on Port 5900;

2. RDP on Port 3389; or

3. ports that are dangerous to expose externally, such as the Samba/SMB protocol (usually found on Ports 139 and 445).

These scans are designed to be non-intrusive and typically have a limited impact on your network. For example, an RDP scan will drop the connection as soon as an 'acknowledgement packet' is returned. This process serves to satisfy the parties that, in this case, RDP is accessible from the internet, and should not cause any disruption to the target endpoint's operation. The process analyses the network perimeter for open ports to highlight any potential vulnerabilities.

Working with Intelligence Providers

Further, insurers may use data on your network footprints and cross-reference against third-party threat sources, with a view to identifying whether or not a breach has occurred. Insurers are able to work with a number of intelligence providers, including law enforcement, to gain insight into vulnerabilities and threats that can lead to serious cybercrime.

You may be reassured to know that when such actions are taken, it is not with the intent to penalise policyholders for vulnerabilities or compromises, but to provide an efficient and valuable service that seeks to prevent future cyberattacks and keep your business safe.

Terminology

Here's an explanation of some of the issues we've used above:

How do ports work?

Computer applications and services use numbered ports (ranging from 1 – 65,000+) to communicate. Each port number allows for computers to differentiate between the different kinds of traffic travelling in a network. For example, general web traffic travels over Port 80 and RDP over Port 3389.

What is an open port?

An open port is a port that is configured to accept packets (a formatted chunk of data sent over a network). For a port to be visible on the internet, an organisation's firewall must be configured to allow external connections through an open port. Typically, ports are only publicly exposed to allow communications from outside of the network, i.e.via the internet. If vulnerable ports are exposed, they may be exploited by cyber attackers.

What is a vulnerability?

A vulnerability is a weakness or flaw in computer software that could allow an attacker to use the software in a way not intended by its creator. Usually, the attacker exploits the flaw to perform malicious and unauthorised actions within the computer system. When vulnerabilities are discovered, they are generally added to a public list of Common Vulnerabilities and Exposures (CVE) and given a CVE ID or number, in the format CVE-2021-12345.

A Collaborative Approach

The above processes are aimed to prevent cyber events and have a positive impact on both a policy holder and the insurer, minimising and mitigating potential threats. When it comes to cyber security and protecting your organisation, it is vital to remain vigilant.

Please do contact our team of experts with any questions, or if you'd like more information. We are ready to help.

Kajal Desor | Associate
T. +44 (0) 20 7933 0207
M. +44 (0) 78 8044 7524
E. **kajal.desor@lockton.com**

Peter Erceg | Senior Vice President
T. +44 (0) 20 7933 2608
M. +44 (0) 77 7646 4370
E. **peter.erceg@lockton.com**