When it comes to network vulnerabilities, how can you ensure critical threats are uncovered without becoming overwhelmed with vast amounts of data? We explore how data can be contextualised to inform a robust Vulnerability Management strategy.
Holes in a Suit of Armour?

Cyber breaches are currently the most feared corporate risk, according to the Allianz Risk Barometer 2019. Holes in the chain-mail of your network may not pose an immediate threat, but sooner or later an ‘arrow’ can find its mark and pierce defences.

Unpatched operating systems, legacy applications and shadow IT all pose potential threats to your networks’ security. The WannaCry ransomware that struck high-profile networks, including the NHS, exploited a Windows vulnerability, to encrypt files, and spread havoc very rapidly across networks in 2017.

Establishing priorities and taking appropriate corrective actions are obvious steps for reducing risk to an appropriate level, and that can only happen once you’ve established a clear picture of your entire network.

But with potential vulnerabilities on a network often running into the tens of thousands, getting a complete view of the landscape and clarifying this into something comprehensible, let alone actionable, is a time consuming and seemingly relentless task. Not only is the myriad of data presented by typical ‘snapshot’ network assessments delivered by vulnerability analysis tools simply overwhelming, it is also just that: a snapshot in time.

With the growth in remote working, one snapshot might only capture 60% of the network while remote workers are disconnected, and networks are changing continually - therefore snapshots offer insufficient value as one-off or irregular activities. Furthermore, processing the data into something meaningful requires specialist knowledge, expertise and dedicated resource.

So how do you move from lack of data or data overload to actionable strategy?
Where are the gaps that could bring down your security? A comprehensive end-to-end process to assess, analyse and remediate vulnerabilities is essential.

An assessment not only allows you to understand the vulnerabilities caused by software, patching, misconfiguration, it also allows you to understand your network in its entirety and detect elements that should or shouldn’t co-exist that may be flying under the radar.

Allowing users connected to your guest Wi-Fi network the ability to view or access your critical infrastructure, for example, could provide a backdoor for a would-be attacker to exploit. Placing these sensitive systems behind a firewall and separating the networks are obvious solutions, but without visibility, this potential loophole may be lying dormant, undetected.

Hackers are looking for holes to exploit, holes that often, nobody in the organisation even knows about. And your ‘armour’ is only as secure as your weakest link, which all too often is your own users.

This is especially true today, when many of the most targeted attacks, such as phishing, are designed to trick users into lowering the defences for attackers.
Cyber breaches are currently the most feared corporate risk

Source: 2019 Allianz Risk Barometer
Most major cyber-attacks can be traced to seemingly minor oversights: an accidentally opened email, an unpatched application, a password innocently shared on a spoofed website.

Prevention through training, and forming good habits for basic data hygiene, are invaluable.

For deeper network vulnerabilities, however, a system to analyse the threat scale and create an actionable strategy is key.

More than a superficial scan, this enables you to determine not only existing threats, but where they exist across your IT estate, providing full visibility of your network and its vulnerabilities. This may include areas you may be currently unaware of, as well as establishing network best practise, for example, in separating networks to control risks.

The Littlefish Vulnerability Quadrant™ can be used to map these vulnerabilities against Volume and Scope, Exploitability and Motivation to evaluate their business significance on a Red, Amber, Green scale in context of the latest cyber security intelligence and the wider threat environment, resulting in an actionable scale of threat matrix.

This brings clarity and understanding to otherwise potentially overwhelming data offering little value without the capacity to surface and analyse it.

About the Author

Littlefish Head of Cyber Security Katy Hinchcliffe, is a highly regarded cyber security leader. With over a decade’s experience delivering a broad range of cyber security services to enterprise clients for global IT outsourcer Capgemini, notably managing the prevent, detect and respond functions on behalf of Rolls-Royce, Katy is now responsible for developing Littlefish’s Cyber Security practice.
The Littlefish Vulnerability Quadrant™

<table>
<thead>
<tr>
<th>Volume and Scope</th>
<th>Evaluation and Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Numeric summary of the extent and scope of the vulnerabilities</td>
<td>The Business significance of the vulnerability – Red, Amber, Green. Green = control methods in place Amber = manage through BAU controls Red = difficult to defend by controls only</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exploitability</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A measure of how exploitable the vulnerability is, on a range from no currently available exploit or difficult to exploit, to highly exploitable by an attacker with exploits currently ‘in the wild’</td>
<td>Assessment of whether the vulnerability leads to only a limited access, relatively unimportant part of the network with low value to an attacker, or allows extensive access, with major consequences and therefore high value to the attacker</td>
</tr>
</tbody>
</table>

The result is a robust and highly focused strategy for assessing new and existing vulnerabilities and a structured plan for remediating them in order of priority.

This delivers a more secure environment informed by market intelligence, conscious of the latest threats in the wider threat environment, via cyber security practitioners connected to threat sharing networks and with access to peer to peer knowledge, reducing organisational risk.

This means less fire-fighting, increases your ability to focus on value-added activity, as well as providing the reassurance that you have the backing of experts to deal with threats and maintain data integrity and compliance with industry best practice standards such as ISO, Cyber Essentials Plus and broader GDPR concerns.
£92m

the total cost to the NHS of the 2017 WannaCry ransomware attack

Source:
2018 ‘Securing Cyber Resilience in Health and Care’ Report
Contact us to learn more about optimising your security investment and risk management strategy through access to the expertise and experience of a cyber security leader:

Littlefish Cyber Security Services
Price House, 37 Stoney Street, Nottingham, NG1 1LS

T: 0115 941 5111
E: sales@littlefish.co.uk