Fighting back against IoT attacks

Following massive web attacks, the security risks in the connected world have been laid bare. By **Vincent Smyth**.

Image: Alamy

The common belief that nothing can be certain, except for death and taxes, can be traced back to the 18th Century. But perhaps the saying needs to be updated for modern times with the addition of age related hearing loss.

To say the Internet of Things (IoT) is here to stay may be the understatement of the decade. We are all knee-deep in the IoT and there is no turning back – gone are the days of thinking connecting refrigerators, security systems and vending machines to the Internet is in a land far, far away.

As this phenomenon grows even stronger, it is more critical than ever that everyone understands how these connected devices are impacting our everyday lives and shifting how we interact with – and even trust – the objects that we have come to rely on daily.

When it comes down to it, the IoT is about devices being controlled by software, connected to the Internet, armed with sensors capable of reporting back to the mothership. We already have cars that are connected to our phones and thermostats connected to our home network, but what we may not consider are the vulnerabilities we risk every time we use a connected device. With Internet-connected devices, there will always be a risk from determined hackers that want to exploit vulnerabilities in a device and the applications that run on it.

It is not just consumers that are concerned; businesses also fear exposing customers to Internet criminals without a way to fix the problem. Indeed, the reputational damage and loss of trust resulting from these break-ins cuts far deeper than the cost of repairing the damage. According to PwC's 2016 Global Economic Crime Survey, executives considered reputational damage the most devastating impact of a cyber breach, followed closely by legal, investment and enforcement costs.

The cost is massive for organisations when a hacker is successful in gaining entry. An organisation's first line of defence to minimise cybercriminal threats should be to shrink the attack surface by decreasing the number of vulnerabilities on its devices. Taking this preventative measure will lower the likelihood considerably that a hacker can do any real harm.

Software vulnerability management

This is why software vulnerability management is so important – it is preventive. Most successful cyberattacks use known vulnerabilities to gain access to corporate IT infrastructures or to escalate privileges once inside them. Once hackers have successfully exploited a vulnerability, they have a base from which to roll out their attack – moving around systems, gathering information and deploying malware – an umbrella term referring to a variety of hostile or intrusive software, including viruses, worms, Trojan horses, ransomware, spyware, adware, scareware and other malicious programs – to steal or terminate business critical information or cause disruption.

"With connected devices, there will always be a risk from determined hackers that want to exploit vulnerabilities." Vincent Smyth

The problem created by vulnerabilities is more broad based than most people – and companies – realise. In Flexera's recently published Annual Vulnerability Review 2016, which presents global data on the prevalence of vulnerabilities and the availability of patches, it was found that, in 2015 alone, 16,081 vulnerabilities were recorded in 2484 products from 263 vendors. These findings illustrate the challenge faced daily by security and IT operations teams trying to protect against security breaches.

However, there are clues in the data that provide insights into how to handle vulnerabilities. Of the 16,081 vulnerabilities discovered, 13.3% were rated as 'highly critical' and 0.5% as 'extremely critical'. Moreover, 84% of vulnerabilities in all products had patches available on the day of disclosure. This means that, by implementing a proper software

vulnerability management strategy, organisations can significantly minimise their attack surface and the likelihood of a successful breach.

Vulnerability intelligence

The first element of that strategy is vulnerability intelligence – referring to all research data on vulnerabilities, including historical data, attack vector, impact, criticality ratings and fixes. Vulnerability intelligence can be integrated with an organisation's security strategy to support risk assessment. It can also be used by software vulnerability management technology to feed and enhance tools.

How is Vulnerability intelligence derived? It begins with investigation to determine whether the numerous vulnerabilities identified globally from countless sources actually exist. Once a vulnerability's existence is confirmed, evaluation of its criticality is vital so the organisation can determine which pose the bigger risk and require more immediate attention.

Vulnerability intelligence feeds into the three critical stages of the software vulnerability management lifecycle.

The lifecycle starts with the 'assess' stage, in which the existence of a vulnerability is researched and verified. Next, the organisation needs to filter out the known vulnerabilities and focus only on those impacting the organisation. That entails comprehensive asset discovery and inventory to determine which systems are potentially threatened by the verified vulnerabilities. Once the universe of known vulnerabilities is winnowed down to the subset impacting the enterprise, then vulnerability intelligence can be applied to determine which are most critical and require prioritised attention.

The second stage of the software vulnerability management lifecycle involves mitigation. This is often where a handoff occurs between the corporate security team and the IT Operations team. However, a 'siloed' approach between security and IT operations is not recommended.

The IT operations team typically handles patch management and will use its application readiness processes to identify and download the applicable patches – remember that 84% of vulnerabilities have patches available on the day of disclosure. The patches then need to be tested – for dependencies, for example – packaged and distributed to the correct machines. This mitigation process must be well managed and automated to avoid system overloads and failures.

The last step of the software vulnerability management lifecycle is verification, whereby the application of the patch or other mitigation technique is verified. Once mitigation is complete, the attack vector for that vulnerability has been eliminated.

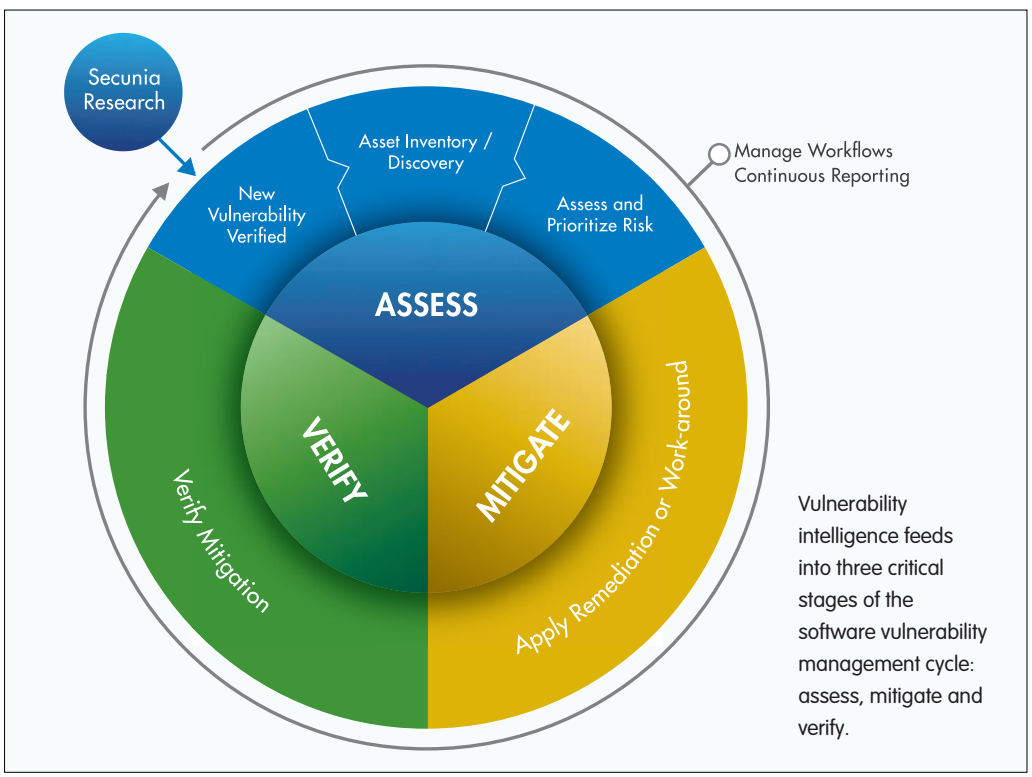
Organisations must be both proactive and reactive in order to fight cybercrime. They must be proactive in order to make it is as difficult as possible for a hacker to break into systems. They must also be reactive, prepared to detect and respond to incidents as they happen.

Many organisations focus on their reactive approaches, dealing only with an attack once it has happened. However, it is exponentially more difficult to identify and respond to breaches when there are too many holes and cracks for hackers to exploit.

A proactive approach via software vulnerability management means investment in the people, processes and technology to lessen the attack surface and minimise the likelihood that a software vulnerability can be exploited in the first place.

We simply can't ignore the fact that our IoT devices are getting smarter. Technology is only going to continue to advance, but as we have seen, innovation almost always comes with inherent risks. Manufacturers and consumers share the burden of taking reasonable precautions to help ensure their devices do not become easy prey for criminals.

Author profile: Vincent Smyth is general manager, EMEA, with Flexera Software.



Vulnerability intelligence feeds into three critical stages of the software vulnerability management cycle: assess, mitigate and verify.