https://securitybrief.asia/story/raw-data-actionable-intelligence-art-and-science-endpoint-security/
From raw data to actionable intelligence: The art and science of endpoint security
28/04/17

ContributorApril 28, 2017 6AM

The endpoint is vulnerable. That's where many enterprise cyber breaches begin: An employee clicks on a phishing link and installs malware, such a ransomware, or is tricked into providing login credentials. A browser can open a webpage which installs malware. An infected USB flash drive is another source of attacks.

Servers can be subverted with SQL Injection or other attacks; even cloud-based servers are not immune from being probed and subverted by hackers. As the number of endpoints proliferate — think Internet of Things — the odds of an endpoint being compromised and then used to gain access to the enterprise network and its assets only increases.

Which are the most vulnerable endpoints? Which need extra protection?

All of them, especially devices running some flavour of Windows, according to Mike Spanbauer, Vice President of Security at testing firm NSS Labs. "All of them. So the reality is that Windows is where most targets attack, where the majority of malware and exploits ultimately target. So protecting your Windows environment, your Windows users, both inside your businesses as well as when they're remote is the core feature, the core component."

Roi Abutbul, Co-Founder and CEO of security firm Javelin Networks, agreed. "The main endpoints that need the extra protection are those endpoints that are connected to the [Windows] domain environment, as literally they are the gateway for attackers to get the most sensitive information about the entire organisation."

"From one compromised machine," he continued, "attackers can get 100 per cent visibility of the entire corporate, just from one single endpoint. Therefore, a machine that's connected to the domain must get extra protection."

Vulnerable IoT and cloud

Scott Scheferman, Director of consulting at endpoint security company Cylance, is concerned about non-PC devices, as well as traditional computers. That might include the Internet of Things, or unprotected routers, switches, or even air-conditioning controllers. "In any organisation, every endpoint is really important, now more than ever with the Internet of Things.

There are a lot of devices on the network that are open holes for an attacker to gain a foothold. The problem is, once a foothold is gained, it's very easy to move laterally and also elevate your privileges to carry out further attacks into the network."

Microsoft, too, takes a broad view of endpoint security: "I think every endpoint can be a target of an attack. So usually companies start first with high privilege boxes, like administrator consoles onboard to service, but everybody can be a victim," said Heike Ritter, a Product Manager for Security and Networking at Microsoft.

Context is everything

Many endpoint security products monitor endpoints and can raise alarms if a breach is detected. Some tools focus on what's happening in this instant; others place incidents in a historical context, so that administrators and security response teams can see only what's going on, but where the problem began.

Online, offline: All endpoints need protection

In an old-fashioned enterprise environment, nearly all endpoints were connected directly to the internal network, and unless they were powered off (like an employee's desktop computer over the weekend), they could be monitors 24/7. What about in today's world, where endpoints are mobile, connected via cellular data or coffee-shop WiFi, or simply offline — but active?

Those endpoints are even more vulnerable when travelling. They must be protected, and monitored by the CISO team so that breaches can be detected and responded to quickly. The same is true for virtual machines that can be spun up and then deactivated at any time. How are they protected?

Finding patient zero

A breach is detected. An endpoint is found to be infected, and is isolated. Yet that endpoint may not the source of the original breach – it may simply be where hacker activity crossed over an alarm threshold. To stop the breach, and prevent it from reoccurring, it's vital to find the root cause of the vulnerability, also known as Patient Zero. That user, device or application can be tricky to identify.

Kowsik Guruswamy, CTO of security firm Menlo Security, said that the data is there to identify breaches, even if technologies like his company's isolation platform stop any harm from being done, or any data from being exfiltrated.

"The best analogy I would tell you is I tell customers that we're giving them a bulletproof vest. So there are no bullets that are going to touch them at all. However, many customers still want to know where the bullets are coming from and what types of bullets are hitting at them. So while we're isolating and making the problem go away, we still use threat intelligence and other techniques, from a purely reporting and forensics perspective, to tell the users what type of bullets came at them."

Solid ideas for endpoint protection

Many companies offer solutions for endpoint protection, whether that endpoint is physical or virtual, mobile or in a data centre or in the cloud. Each company has a different vision. For example, Javelin Networks focuses on protecting Active Directory, an essential component of a Windows domain network. Active Directory can be used by hackers to learn about network resources, and target future attacks.

Protect the endpoints. Or else.

Every endpoint represents a potential enterprise vulnerability. Mobile phone, notebook computer, data centre server, virtual container in the cloud, the IoT, and even industrial equipment. It's not a question of "if" endpoints will be attacked, but "when." The challenge for enterprises is to be able to prevent, detect

and respond to those breaches. The technologies and service providers above have answers. It's time more organisations talked to them.

Article by Alan Zeichick, freelance technology writer.