BIZCOMMUNITY

Survey reveals 7 uncomfortable truths of endpoint security

A global survey, 7 Uncomfortable Truths of Endpoint Security, reveals that IT managers are more likely to catch cybercriminals on their organisation's servers and networks than anywhere else.

Source: pixabay.com

Sophos, a global provider network and endpoint security, recently announced the findings of its global survey, 7 Uncomfortable Truths of Endpoint Security, which reveals that IT managers are more likely to catch cybercriminals on their organisation's servers and networks than anywhere else.

Where are cyber attacks taking place?

In fact, IT managers discovered 37% of their most significant cyber attacks take place on their organisation's servers and 37% on its networks. Only 17% were discovered on endpoints and 10% were found on mobile devices.

Whereas for South African IT managers, 42% of the most significant cyber attacks were discovered on their organisation's servers, 33% on their networks, 20% on their endpoints and 5% on mobiles. The survey polled more than 3,100 IT decision makers from mid-sized businesses in 12 countries including the US, Canada, Mexico, Colombia, Brazil, UK, France, Germany, Australia, Japan, India, and South Africa.

“Servers store financial, employee, proprietary, and other sensitive data, and with stricter laws like GDPR or POPI that require organizations to report data breaches, server security stakes are at an all-time high. It makes sense that IT managers are focused on protecting business-critical servers and stopping attackers from getting on the network in the first place and this leads to more cybercriminal detections in these two areas,” said Chester Wisniewski, principal research scientist, Sophos.

“However, IT managers can’t ignore endpoints because most cyber attacks start there, yet a higher than expected amount of IT managers still can’t identify how threats are getting into the system and when.”

Twenty-six percent of South African IT managers who were victim to one or more cyber attacks last year can’t pinpoint how the attackers gained entry, and 18% don’t know how long the threat was in the environment before it was detected, according to the survey. To improve this lack of visibility, IT managers need endpoint detection and response (EDR) technology that exposes threat starting points and the digital footprints of attackers moving laterally through a network.

“If IT managers don’t know the origin or movement of an attack, then they can’t minimize risk and interrupt the attack chain to prevent further infiltration,” said Wisniewski. “EDR helps IT managers identify risk and put a process in place for organizations at both ends of the security maturity model. If IT is more focused on detection, EDR can more quickly find, block and remediate; if IT is still building up a security foundation, EDR is an integral piece that provides much-needed threat intelligence.”

On average, South African organisations that investigate one or more potential security incidents each month spend 36 days a year (three days a month) investigating them, according to the survey. It comes as no surprise that regional IT managers ranked identification of suspicious events (31%), alert management (22%) and ability to search on file attributes (12%) as the top three features they need from EDR solutions to reduce the time taken to identify and respond to security alerts.

“Most spray and pray cyberattacks can be stopped within seconds at the endpoints without causing alarm. Persistent attackers, including those executing targeted ransomware like SamSam, take the time they need to breach a system by finding poorly chosen, guessable passwords on remotely assessible systems (RDP, VNC, VPN, etc.), establish a foothold and quietly move around until the damage is done,” said Wisniewski.

“If IT managers have defense-in-depth with EDR, they can also investigate an incident more quickly and use the resulting threat intelligence to help find the same infection across an estate. Once cybercriminals know certain types of attacks work, they typically replicate them within organizations. Uncovering and blocking attack patterns would help reduce the number of days IT managers spend investigating potential incidents.”

Implementing EDR solutions

Fifty-six percent of respondents from South Africa said they were planning to implement an EDR solution within the next 12 months. Having EDR also helps address a skills gap. Seventy-five percent of IT managers wish they had a stronger team in place, according to the survey. More information is available in the 7 Uncomfortable Truths of Endpoint Security PDF and on Sophos News

The 7 Uncomfortable Truths of Endpoint Security survey was conducted by Vanson Bourne, and is available for download. (PDF File. Size: 879KB)