REDUCE STRATEGIC RISK BY RETHINKING YOUR ENDPOINT SECURITY

Unrelenting breaches of sensitive data are driving aggressive scrutiny and increasing penalties from regulators. Enterprises can confront this strategic risk by focusing on the primary point of contact between attackers and critical data: endpoints.

EXECUTIVE SUMMARY

Organizations face strategic risks related to data stored or processed on laptops, workstations and servers, also known as endpoints. These risks are driven by four key trends:

- Increasing regulatory scrutiny of information security measures including penalties for inadequate implementation
- Well-resourced independent and state-supported actors developing exploits against widely used trusted software, giving attackers rapid, widespread access to vulnerable networks
- Ransomware attacks that include extortion demands to retrieve stolen data or prevent its disclosure
- Growing incentives for insiders to participate in externally driven cyberattacks.

These trends combined mean large organizations can unexpectedly incur enormous costs due to regulatory penalties, external breaches or insider attacks. Securing endpoints has always been important but it's only getting more critical as risks grow and evolve.

Organizations can reduce the risks they face by making specific improvements to their endpoint security. Recent advances in technology have made it possible for security teams to quickly detect malicious events and conduct proactive investigations to prevent them from becoming catastrophic.

COMMON THREAT SCENARIOS

External cyber attacker:

- Steals data to sell it for profit
- Steals data to extort a ransom payment
- Encrypts data to extort a ransom payment
- Encrypts data to debilitate the organization.

Internal authorized user:

- Steals intellectual property (IP) or personally identifiable information (PII) to sell or commercialize it
- Executes fraudulent transactions for personal gain
- Steals IP at the behest of a third party such as a prospective employer
- Publicizes information to embarrass the organization.

INDICATORS OF GROWING RISK

In its 2021 Global Business Risk Barometer, global insurer Allianz found cybersecurity incidents were the third highest risk faced by businesses, after only business interruption and the COVID-19 pandemic.[1]

Organizations that hold customer data or intellectual property must contend with growing efforts to capitalize on their information. A 2019 report by the US Department of Homeland Security found "the cyber threat landscape is distinguished by an expanding set of actors" and attributed this to the "low barrier of entry for new actors" and the diffusion of expertise from former government and intelligence operatives and commercial practitioners to threat actors.[2]

Copyright ©2023 Nuix. All rights reserved.

We find seven recent events illustrate the risk environment today.

REGULATORY RISK

- In July 2019 Equifax agreed to pay at least $575 million for failing to take "reasonable steps" to secure its network. Regulators found Equifax culpable for failing to prevent a data breach that affected 147 million people.[3]
- In October 2020, the UK Information Commissioner's Office (ICO) fined British Airways £20 million, ICO's largest fine to date. ICO concluded British Airways had failed to protect customer data that was compromised in a 2018 cyberattack.[4]

INSIDER THREAT RISK

- In August 2020, an engineer at carmaker Tesla was approached by a Russia-based ransomware group, which offered him $1 million to execute ransomware on his work computer.[5] Though he declined to participate, the story revealed the incentives external actors offer insiders.
- In August 2021, the black market price of a domain administrator credential to an attractive ransomware target organization was 12 BTC, or about $590,000 according to a report by KE-LA.[6] This implies a tremendous incentive for system administrators to sell usernames and passwords.

CYBER THREAT RISK

- In December 2020, a US Cybersecurity and Infrastructure Security Agency (CISA) Emergency Directive revealed that SolarWinds Orion products were currently being exploited by malicious actors.[7] At least 18,000 SolarWinds customers worldwide were affected; over 200 were actively targeted in attacks initiated from malware included in an apparently legitimate update to the Orion product.
- In March 2021 Microsoft announced a series of vulnerabilities in Microsoft Exchange. Attacks on these vulnerabilities, dubbed Hafnium , allowed remote control of compromised Exchange servers and affected 21,000 organizations worldwide.[8]
- In May 2021, a ransomware attack on Colonial Pipeline resulted in a shutdown of the company's entire gasoline pipeline system.[9]

Taken together, these events place the modern enterprise in an uncomfortable squeeze between regulators and internal and external threat actors.

WHAT IT MEANS FOR YOU

These trends carry four key implications for organizations..

1. Regulators are closely scrutinizing breach victims' information security programs and imposing fines. One study found fines for breaches of the European Union's General Data Protection Regulation (GDPR) rose by nearly 40% between January 2020 and January 2021.[10] The US Federal Trade Commission's complaint against Equifax alleged twelve shortcomings in its security program, including that it failed "to monitor or log privileged account activity across numerous systems."[11] The ICO's penalty notice to British Airways alleged the airline's failure to apply automated application blocking contributed to the breach.[12] In the past, regulators might have overlooked these shortcomings. Now they're the basis for significant fines.

   You can reduce the risk of regulator-induced pain by implementing technologies for automated breach prevention and rapid detection and response, and demonstrating vigilance in your security programs.

2. Compromising legitimate software updates gives attackers instant, global-scale access. The group behind the SolarWinds attack compromised the Texas software company's update infrastructure. This allowed the cybercriminals to deploy malware to some 18,000 systems worldwide. Some affected organizations had to examine dozens of SolarWinds servers for evidence of compromise, and incident response firms worldwide were overwhelmed by demand. In the case of Hafnium, the cyberattackers used a similar method to install malware in on-premises Microsoft Exchange servers.

   In both cases, industry and government agencies provided valuable threat intelligence in the form of IP addresses, file hashes, command lines and other indicators. Enterprises that could efficiently search for and detect these indicators found and evicted the attackers.

   These examples dramatically illustrate why you need the ability to conduct large-scale cybersecurity investigations at speed.

3. Ransomware attacks are expanding in scope and leading to longer attacker dwell time. While earlier ransomware attacks were primarily aimed at making money by demanding a fee to decrypt the data, some recent incidents have featured extortion to prevent the release of sensitive or compromising information.

   Obtaining that information requires the attacker to be present on your network for some time, giving network defenders an opportunity to detect and evict them before they can find your dirty laundry.

4. The incentives for authorized insiders to cooperate with external attackers are growing. The effort to coopt a Tesla engineer illustrates cyberattackers' willingness to target insiders. At the same time, there is a growing cadre of specialist cybercriminals who focus on acquiring network credentials – which are trivial for system administrators to acquire – and selling them on the black market to ransomware operators.

   These evolving incentives represent a good reason to monitor employees who have access to sensitive data, particularly privileged users.

Copyright ©2023 Nuix. All rights reserved.

RISK REDUCTION STARTS WITH ENDPOINTS

The inability to secure the endpoints – laptops, desktops, servers, virtual machines and increasingly mobile devices – employees use to store and process critical information is a substantial risk driver. This capability gap makes it harder to prevent risks directly but also raises a challenge if you need to demonstrate regulatory compliance. Historically, organizations have relied heavily on two endpoint technologies to manage risk: antivirus software and data loss prevention (DLP) products.

ANTIVIRUS

Antivirus software is an important layer of defense against common malware. However, many modern attacks don't use traditional malware. External attackers – particularly the ones that are likely to be strategic threats – often prefer to compromise utilities that are already in the target environment, also called "living off the land."

Antivirus products have a hard time detecting malicious use of these tools. Antivirus tools also can't protect against malicious behavior by authorized users.

DATA LOSS PREVENTION

DLP can help detect attempts by malicious insiders to exfiltrate sensitive data. However, they cover only one portion of the insider threat kill chain: the final movement of data off the endpoint. They generally don't analyze user behavior more broadly, which means they don't detect other insider activities such as manipulating documents, staging information in preparation for theft and using file sharing or secure chat applications to move data outside the corporate network.

Risks from authorized users also go beyond data theft. Behaviors such as discrimination, harassment and substance abuse are usually at odds with enterprise values. Protecting employees from a hostile work climate assures their wellbeing and shields the organization from costly complaints and lawsuits.

The current prevalence of remote work also causes visibility gaps for security teams, who rely on network-level tools to detect and investigate threats. Many network monitoring tools aren't effective if employees are primarily working from home.

CRITICAL QUESTIONS

Organizations seeking to drive down strategic risk by improving their endpoint security should ask these four key questions:

1. How good is our visibility? Most security teams have a limited understanding of what is happening on their endpoints. However, you need to know what is happening on any given system at any time, even when there is no alert. This visibility requirement spans system, network and user activity. Having good visibility isn't just about tooling; you also need the expertise to interpret the data the tools provide.
2. Can we investigate our systems both broadly and deeply? Future supply-chain compromises such as the SolarWinds and Hafnium scenarios will require security teams to quickly examine dozens or even hundreds of systems for newly revealed indicators of compromise. You will need to perform this task quickly and efficiently, and seamlessly move into a deeper forensic examination if you detect any issues.
3. Can we detect the subtle threat indicators without being overwhelmed by noise? The trouble with detecting insider threats is differentiating innocuous activity from unauthorized use. The differences are subtle and require the ability to understand complex combinations of behaviors. Similarly, advanced external attacks can be detected with behavior indicators like those in the MITRE ATT&CK framework but this also requires you to tune out false positives, quickly and at scale.
4. How flexible is our detection? Rapid changes in threat activity, IT infrastructure and the nature of work itself mean that security teams constantly face new threat scenarios. Often, security teams are forced to wait on vendors to detect the threats that most concern them. In some cases, those detections come too late or simply never rise high enough in the vendor's priority list. You need flexible tools that adapt their posture to detect the behaviors that concern you most.

BALANCING RISK MANAGEMENT AND EMPLOYEE PRIVACY

Monitoring employee behavior on the endpoint can be seen as intrusive or raise privacy concerns. Organizations can respect and support employee privacy by:

- Maximizing the use of routinely collected endpoint telemetry to triage alerts
- Focusing on protecting the enterprise and the jobs of employees
- Targeting specific areas of user misconduct rather than general user activities
- Engaging with key stakeholders across the enterprise in building a user monitoring program, including legal and human resources
- Conducting clear employee education and awareness efforts about the program.

Copyright ©2023 Nuix. All rights reserved.

CHANGING YOUR MINDSET

Endpoints present a broad and rich target for attackers seeking to profit from or damage the modern enterprise. Enhancing endpoint security gives you the ability to detect and prevent major data breaches, thereby avoiding regulatory scrutiny and severe penalties. It also allows you to detect and intervene with malicious insiders before they evolve into serious threats.

Deepening the security of your endpoints requires a shift in posture and mindset, in which you augment preventive technology with comprehensive awareness of what is happening on your network and the ability to rapidly evolve your detection posture. Organizations that master these capabilities will decrease a critical risk and gain competitive advantage over those that do not.

ABOUT THE AUTHOR

HOKE SMITH – VICE PRESIDENT, CYBERSECURITY

Hoke implements cybersecurity and insider threat detection and response solutions for Nuix customers. He has more than 20 years' experience solving complex technical problems for large organizations. Before joining Nuix, he worked on insider threat and big data analytics programs at IBM, primarily for defense and intelligence organizations. His areas of expertise include endpoint security, counterintelligence, insider threat detection, optimizing organizational performance and big data analytics.

REFERENCES

1. *Allianz, Allianz Risk Barometer, 2021.*
2. *Department of Homeland Security, Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar, 2019.*
3. *Federal Trade Commission, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach, July 22, 2019.*
4. *Information Commissioner's Office, ICO fines British Airways £20m for data breach affecting more than 400,000 customers, October 16, 2020.*
5. *ClearanceJobs, Tesla Insider Works with FBI to Turn the Tables on Russia's Million Dollar Attempt to Hijack the Network, August 26, 2020.*
6. *KELA, All Access Pass: Five Trends with Initial Access Brokers, August 2, 2021.*
7. *Department of Homeland Security, Emergency Directive 21-01, December 13, 2020.*
8. *Security Boulevard, Timeline of a Hafnium Attack, May 5, 2021.*
9. *Bloomberg, Hackers Breached Colonial Pipeline Using Compromised Password, June 4, 2021.*
10. *DLA Piper, DLA Piper GDPR Data Breach Survey 2020, January 20, 2020.*
11. *Federal Trade Commission, United States District Court for the Northern District of Georgia Atlantic Division Document 2361, July 22, 2019.*
12. *Information Commissioner's Office, Penalty Notice Section 155, Data Protection Act 2018, Case ref: COM0783542, October 16, 2020*

nuix

Nuix (www.nuix.com, ASX:NXL) creates innovative software that empowers organizations to simply and quickly find the truth from any data in a digital world. We are a passionate and talented team, delighting our customers with software that transforms data into actionable intelligence and helps them overcome the challenges of litigation, investigation, governance, risk and compliance.

APAC
Australia: +61 2 8320 9444

EMEA
UK: +44 203 934 1600

NORTH AMERICA
USA: +1 877 470 6849

Nuix (and any other Nuix trademarks used) are trademarks of Nuix Ltd. and/or its subsidiaries, as applicable. All other brand and product names are trademarks of their respective holders. Any use of Nuix trademarks requires prior written approval from the Nuix Legal Department. The Nuix Legal Department can be reached by e-mail at Legal@nuix.com.

THIS MATERIAL IS COMPRISED OF INTELLECTUAL PROPERTY OWNED BY NUIX LTD. AND ITS SUBSIDIARIES ("NUIX"), INCLUDING COPYRIGHTABLE SUBJECT MATTER THAT HAS BEEN NOTICED AS SUCH AND/OR REGISTERED WITH THE UNITED STATES COPYRIGHT OFFICE. ANY REPRODUCTION, DISTRIBUTION, TRANSMISSION, ADAPTATION, PUBLIC DISPLAY OR PUBLIC PERFORMANCE OF THE INTELLECTUAL PROPERTY (OTHER THAN FOR PREAPPROVED INTERNAL PURPOSES) REQUIRES PRIOR WRITTEN APPROVAL FROM NUIX.

Copyright ©2023 Nuix. All rights reserved.