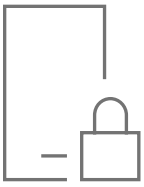
Microsoft Security

Keeping up with a changing cybersecurity landscape

Contents

Introduction

Most of all, CISOs must deal with a cybersecurity landscape of increasing complexity.



A CISO's role has never been easy, but it seems to be getting more challenging every day. The job description is pretty full:

- ✓ protect the organisation's digital assets
- ✓ promote good security practices throughout the business
- ✓ understand the needs and risks of individual business units
- ✓ regularly engage with C-suite peers and the board of directors to help them strategically manage risk

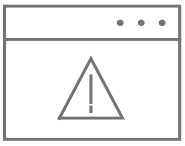
Most of all, CISOs must deal with a cybersecurity landscape of increasing complexity. The days of securing assets behind a fortified perimeter are long gone. Data resides in the cloud, in endpoints, and across the supply chain, greatly expanding the attack surface.

And now, CISOs must deal with the new realities of work created by a global pandemic. A world in which entire workforces were suddenly required to work from home raises the stakes significantly for securing endpoint devices, data and network infrastructure.

It's critical, therefore, for CISOs to stay current on emerging threats and most importantly, how threat protection strategies are evolving to help keep organisations secure.

Emerging threats

Many online bandits are attracted to a newer generation of 'malware free' attack techniques.



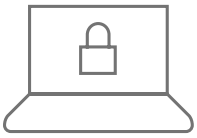
Just as the shortest distance between two points is a straight line, cyber criminals will spend the least amount of sweat equity necessary to compromise systems and exfiltrate data. So it shouldn't surprise anyone that many online bandits are attracted to a newer generation of 'malware free' attack techniques. Why write malware when you can penetrate a system with code executed from memory or compromised credentials?

"I've been brought in to more than one breach where the attacker used malware-free approaches like password guessing against a remote desktop to first gain access to the environment," said Chris Clements, vice president of solutions architecture at Cerberus Sentinel, a cybersecurity consultancy. "The attackers then used built-in system functions to escalate their privileges and give them complete control over all systems and data on the network."

These attacks can be devastating," Clements added, **"as the attackers are mimicking the same activities as legitimate IT administrators that anti-virus isn't designed to stop."**

Advanced phishing techniques

Phishing remains a popular threat, with threat actors adopting advanced tactics to avoid traditional network defences.



Phishing remains a popular threat, with threat actors adopting advanced tactics to avoid traditional network defences. They're hiding behind packet obfuscation, encryption, multi-phased payloads and fast flux DNS, where botnets hide phishing delivery sites behind a network of compromised hosts acting as proxies.

Ransomware attacks are also evolving. The more sophisticated operators will penetrate a target, then look for a partner who can deploy their ransomware into the target in a customised fashion. For example, developers of the LockerGoga ransomware, which needs administrative rights to execute, have been known to so thoroughly analyse a target's defences that they don't even bother to hide their bad app because they know those defences won't detect it.

Attackers are also using tools already installed on a system, such as PowerShell, to spread on a network and broaden infestation. These intruders 'live off the land' once they penetrate a system, using publicly available tools and utilities to accomplish their ends. These attacks are difficult to detect because to defenders they appear to be normal network activity.

Rising remote exploits

According to KnowBe4, a security awareness provider, email attacks related to the coronavirus were up 600% during the quarter that ended 30 March, 2020.

As more employees are forced to work from home due to the COVID-19 epidemic, remote workers pose another heightened vulnerability to organisations. The suddenness of the shift to remote work for many organisations left many security teams playing catch-up to ensure proper policies and protections were in place. Not surprisingly, bad actors are also exploiting the pandemic via social engineering. According to KnowBe4, a security awareness provider, email attacks related to the coronavirus were up 600% during the quarter that ended 30 March, 2020.

"The bad guys are opportunists and they will use every chance they get to take advantage of people's heightened emotions during crisis situations such as this one by trying to entice them to click on a malicious link or download an attachment laced with malware," said KnowBe4 CEO Stu Sjouwerman.

Beleaguered defenders

The expanding threat landscape puts more pressure on CISOs to modernise security operations to reduce inefficiencies.

The expanding threat landscape puts more pressure on CISOs to modernise security operations to reduce inefficiencies, increase visibility across the organisation and become more proactive in identifying and protecting against threats.

Security teams have traditionally been tasked with monitoring specific domains, without interaction or integration. These silos can prevent defenders from seeing the full context of an attack until it's too late. Today's attackers move so quickly that by the time SecOps teams recognise the full extent of an issue, their systems may have already been compromised.

This challenge is exacerbated by an ever-increasing mix of security products and services. Typically, these products use different portals, data schema and methodologies. Monitoring data across those products manually can delay response times and even miss elements of an attack itself.

An increase in security products and the data they collect and analyse often creates alert fatigue. Security analysts can't possibly prioritise the volume of alerts they receive to address the biggest threats. All the intelligence they're collecting is not actionable. Without the right tools to help them respond proactively, before or as a breach is occurring and to block persistent threats, defenders are at a distinct disadvantage when battling adversaries.

A new era of threat protection

Identity-based security is a key component of an emerging security framework known as Zero Trust.

Threat protection is evolving to address these challenges, with emerging methods and technologies designed to fortify traditional defences.

For example, network controls have begun to take a back seat to identity as a means to protect systems and data. When the defence paradigm centred on the perimeter and IT architecture shared a common IP address range, security controls were network oriented. As the cloud and mobile platforms have taken data outside the perimeter, security protections also must extend outside the network. As a result, organisations are exploring ways to retool their defences around context and identity.

With the perimeter paradigm, once you logged into a system, you were considered 100% trusted. With the identity paradigm, access to a system is limited to what the user needs to do their job, and any anomalous behaviour will trigger alerts. Identity-based security is a key component of an emerging security framework known as Zero Trust. This model is based on the premise that trust should not be given to anything inside or outside the organisation. Everything needs to be verified before accessing anything.

More tools for in-depth defence

Security teams now have the ability to deploy advanced 'hunting' capabilities to root out sophisticated breaches.

Modern threat protection requires security controls that continuously cross-correlate and analyse relevant variables in near real time and decide whether an identity should be granted or denied access. This need is increasing the urgency for organisations to adopt automation, artificial intelligence (AI) and machine learning (ML) across their security stacks.

AI and ML play critical roles across cybersecurity operations because they make it possible to analyse massive amounts of data for suspicious activity patterns and threat signals that human analysts can't possibly see until it's too late. ML algorithms can turn raw data from multiple sources into incidents that give defenders the kind of visibility they need to understand the entire context of an attack and craft a targeted response.

AI, ML and automation also help organisations become less reactive and more proactive in identifying and responding to threats. Security teams now have the ability to deploy advanced 'hunting' capabilities to root out sophisticated breaches or better understand how their organisation's assets behave. This approach increases an organisation's ability to defend against persistent attacks and block attackers from gaining a foothold to exploit data and systems.

The CISO's job isn't getting easier. But with a clear view of the changing cybersecurity landscape and access to evolving defence methods, their nights may be a little more restful.

Learn more about how AI, automation and integration help keep users, endpoints, cloud apps and data secure.

Microsoft