IT Faces New Security Challenges in Wake of COVID-19

IT Faces New Security Challenges in Wake of COVID-19

Cybercriminals never met a tragedy they couldn't exploit. These same creeps are now using COVID-19, or Coronavirus, to sneak their way into YOUR network. The pandemic ups the security ante, as hackers are launching new phishing and ransomware attacks exploiting Coronavirus fears.

On top of new threats, enterprises are moving at lightning speed to remote work, something they are not used to. There are myriad training, adoption and security issues that must be addressed for this remote work to be safe and productive.

Here are new security issues detailed by the Cybersecurity and Infrastructure Security Agency, or CISA, as well as the United States Computer Emergency Readiness Team, or CERT:

- Phishing
- Unpatched Obsolete Devices Ripe for Picking
- Ransomware
- Scams
- Malicious E-mail, Especially Containing COVID-19 Subject Lines

We are covering nine security issues raised by COVID-19/Coronavirus, along with how CoreView addresses each.

On top of new threats, enterprises are moving at lightning speed to remote work, something they are not used to.

1. Email Safety in Wake of COVID-19

Scams are exploding, with hackers posing as charities or other COVID-19-related organizations. "The Cybersecurity and Infrastructure Security Agency (CISA) warns individuals to remain vigilant for scams related to Coronavirus Disease 2019 (COVID-19). Cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes," the agency warned. "Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19."

Here are some key CISA email tips:

- "Avoid clicking on links in unsolicited emails and be wary of email attachments. See Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams for more information.
- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity's authenticity before making donations. Review the Federal Trade Commission's page on Charity Scams for more information."

How CoreView Enforces O365 Email Safety

E-mail is the most common way hackers breach your systems, so insecure mailboxes and poor e-mail user practices are perhaps your biggest security exposure. Mailboxes are made vulnerable through insecure, weak and never expiring passwords, as well as a lack of multi-factor authentication (MFA).

Meanwhile, monitoring employee activities such as their mailbox practices can identify risky behavior and proactively secure business-critical data. Preventing risky activities such as auto-forwarding to external email addresses and limiting access rights to other user's mailboxes can prevent the spread of malware and the leakage of data through emails. In addition, being aware of unusual email activity prevents targeted spam or social engineering tactics common among today's cybersecurity threats.

Key rules applied to mailbox security relate to access rights. CoreView flags user accounts with anomalous permissions such as access rights to more than five other user mailboxes, accessing mailboxes of other departments, disabled accounts able to access mailboxes and more. These are not for Room, Shared, or Team mailboxes, but rather actual User Mailbox accounts. Users who have this type of advanced access rights to other users' mailboxes should be investigated to ensure they are being used for acceptable business purposes.

Often, mailbox security can be compromised by spam and malicious malware. CoreView can discover instances of malware sent from your organization via e-mail – and track this spread in minute detail.

CoreView flags user accounts with anomalous permissions such as access rights to more than five other user mailboxes, accessing mailboxes of other departments, disabled accounts able to access mailboxes and more.

2. Ransomware and Malware Explosion

Ransomware remains a top hacker technique. Now cybercriminals are posing as COVID-19-related charities and organizations enticing the unwitting into clicking malicious links. "Ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our nation's networks, locking up private sector organizations and government agencies alike. And that's only what we're seeing – many more infections are going unreported, ransoms are being paid, and the vicious ransomware cycle continues on," CISA explained. "We strongly urge you to consider ransomware infections as destructive attacks, not an event where you can simply pay off the bad guys and regain control of your network (do you really trust a cybercriminal?)."

"Many more infections are going unreported, ransoms are being paid, and the vicious ransomware cycle continues on," CISA explained.

Here is CISA's ransomware advice:

1. "Update and patch systems
2. Make sure your security solutions are up to date
3. Review and exercise your incident response plan
4. Pay attention to ransomware events and apply lessons learned
5. Practice good cyber hygiene; backup, update, whitelist apps, limit privilege, and use multifactor authentication
6. Segment your networks; make it hard for the bad guy to move around and infect multiple systems"

How CoreView Tackles Ransomware and Malware

To deal with ransomware, you must:

- Implement strong password policy and MFA
- Limit granting of administrative access and privileges, and achieve network segmentation via Role-Based Access Control (RBAC)
- Perform audit-based forensics on how ransomware and other malware spread

Malware often gets through anti-virus/anti-malware defenses, especially zero day attacks. CoreView provides auditing tools for cloud operations. CoreView shows you every single file accessed, and every single action taken by an administrator or a user since they had a security event on one of their devices. That is how we prevent malware

like ransomware from going on, and on, and on, and on – spreading throughout the organization. We proactively see and report on what was touched and then do a deeper dive analysis on those actions.

By speeding up security audits and performing more efficient forensic analysis, IT quickly closes any security issues when they are identified. Finding the audit trail to identify these types of attacks is extremely difficult, and requires assistance from specialized tools that have powerful security auditing and analysis capabilities – like those offered by CoreView.

3. Danger of Unpatched and Out-of-Date Devices

Most successful breaches are against unpatched or legacy computers. Keeping devices updated is critical to proper cybersecurity. "Adversaries operating in cyberspace can make quick work of unpatched Internet-accessible systems," CISA warned. "Many organizations lack robust patch and configuration management policies and procedures to guide the coordination of vulnerability management-related activities at an operational level."

Patches act as blue prints for hackers who reverse engineer the vulnerability identified by the patch, and launch attacks knowing many devices will not be updated – making them sitting ducks. It is taking less and less time for these attacks to appear. "Moreover, the time between an adversary's discovery of a vulnerability and their exploitation of it (i.e., the 'time to exploit') is rapidly decreasing. Industry reports estimate that adversaries are now able to exploit a vulnerability within 15 days (on average) of discovery. After gaining entry into information systems and networks, these adversaries can cause significant harm."

Even enterprise computers are not always updated, and are regularly attacked. "Historically, most vulnerabilities identified by CISA are related to unsupported operating systems that cannot receive patched or upgraded (secure) software. This is largely due to the prevalence of legacy systems across all industries and sectors, some of which perform mission critical functions. The continued presence of end-of-life (EOL) systems is mostly due to the budgetary constraints inherent in replacing large amounts of EOL systems, often at the reduced funding levels of sub-organizations," CISA said.

Patches act as blue prints for hackers who reverse engineer the vulnerability identified by the patch, and launch attacks knowing many devices will not be updated – making them sitting ducks.

How CoreView Insures Patched and Up-to-Date Devices

During this crisis, many employees are working from home, still just miles from the office. In other cases, workers leave the area, going to vacation homes, living with friends or relatives, fleeing the hardest hit zone. There is no telling what devices they use for work, and to connect to the corporate network. While a productivity boost, all these devices are a security nightmare.

IT should know exactly what these devices are for several reasons. Systems are only secure if they are patched and using up-to-date modern software, including operating systems. Windows XP does not rate as a high security platform! What is the OS, what is the patch status? Is the device safe?

Mobile devices have the same concerns. What kind of OS is running? Is it up to date?

Keeping software patches and anti-virus tools up to date requires that IT knows, and can validate the configuration of workstations, laptops and mobile devices, and what software is installed. More to the point, how do you know if the device is infected? And if it is, how do you know what that device did to potentially spread malware or other malicious software?

Keeping software patches and anti-virus tools up to date requires that IT knows, and can validate the configuration of workstations, laptops and mobile devices, and what software is installed.

4. Decentralization without Security and Control Leads to Chaos

CISA sees network segmentation as making systems more vulnerable. If a hacker cannot break into one network segment, he can go after another not as well protected. "The decentralization of organizations and their governance processes makes it difficult to coordinate the remediation of vulnerabilities. Network owners should be aware of who is operating their respective networks, if not done in-house," CISA said.

This same theory applies to end user access rights, which are too often overly broad and deep. Did you know that 80% of SaaS breaches involve privileged permissions? And that admins have the most privileges of all?

How CoreView Segregates and Secures Your Tenant

With CoreView, you can segregate your operator responsibility by implementing a granular RBAC – but first ask yourself:

- Why is Segregation of Duty a must-have for your organization?
- What are the regulatory constraints?
- What is the risk if you do not implement it?
- What is the business impact to not implementing it?

CoreView addresses these pain points with our Role-Based Access Control (RBAC) features that give you fine-grained control over what admins can, and cannot do.

5. Stopping Breaches

Ponemon's 'Cost of a Data Breach' Survey explains the damage of data breaches. What is the cost of losing a file? They say $141. The average cost to an enterprise of a breach -- $3.62 million. It is about 191 days on average to figure out that you have had a data breach.

How CoreView Helps Stop Breaches

The best defense is stopping breaches before they happen. From a prevention standpoint, CoreView has a global suspicious sign-in attempt map showing not only what IP address hackers were attacking from and failed, but also what accounts they went after. It also shows if the configuration included multifactor authentication or not, and whether or not conditional access policies were effective for a specific attempt. Finally, it details the end-result of the sign-in attempt.

From a prevention standpoint, CoreView has a global suspicious sign-in attempt map showing not only what IP address hackers were attacking from and failed, but also what accounts they went after.

6. How Did a Breach Happen?

Breaches sometimes bust through the best barriers. Moreover, most IT shops discover the incursion months or even over a year after it happened. How then do you figure out how and why it happened?

How CoreView Performs Breach Forensics and Discovers Attack Path

The answer is forensics that rely on long-term log retention so you can perform a proper security audit. Here you discover what happened so you can minimize ongoing damage, and by finding the source, stop it from happening again.

Once a data breach or malware infection occurs, you need to find out everything about it. CoreView, though, quickly gets to the heart of the matter. A CoreView-enabled administrator can choose 'file access' and see all the files, the names, and the paths to the files that were accessed after the breach or malware attack.

7. IT Insiders as the Enemy

How CoreView Segregates and Secures Your Tenant

A common assumption many have is that IT, which controls the infrastructure, apps and data, is inherently trustworthy.

Too often those in IT blindly trust others in IT, and give these workers higher level privileges than they need, and which can be used to abuse access to corporate and personal information. According to a survey by Cyber-Ark, a third (35%) of IT pros spy on other company employees.

A sizeable portion of insider breaches come from technical staff: 6% from developers and another 6% from admins, according to the Verizon Data Breach Investigations Report. Many insider incursions result from privilege abuse, though there are many other ways IT abuses its access.

Too often those in IT blindly trust others in IT, and give these workers higher level privileges than they need, and which can be used to abuse access to corporate and personal information.

According to a survey by Cyber-Ark, a third (35%) of IT pros spy on other company employees.

How CoreView Blocks Insider IT Malfeasance

The first defense is using RBAC to only grant privileges that are absolutely needed, and only for the time these privileges are absolutely needed for. At the same time, have a system for tracking admin activities and let admins know tracking is in place. This alone can ward off many dangers.

8. Employees as the Enemy

The Verizon report finds that 14% of breaches come from insiders. Insiders are more dangerous than most outsiders are. Insiders are already on the network, and sometimes with high-level privileges.

To fight off the insider threat, you need a full approach to security, along with the ability to address Office 365-specific vulnerabilities.

A key issue is knowing what is going on in the network and controlling dangerous activity.

Verizon advises IT to implement strong access controls and provide access levels fitted to true needs, trust, and levels of responsibility. "Having identified the positions with access to sensitive data, implement a process to review account activity when those employees give notice or have been released," Verizon suggested.

How CoreView Blocks Employee Malfeasance

The answer is to identify internal and external threats to your environment -- then step up your defenses. Here, CoreSecurity alerts give you an early warning system for internal and external threats to your Office 365 environment, so you can identify and defend yourself against security breaches before they occur.

As much as cybercriminals around the world attack government systems, insiders can be a more insidious threat. Often this is through social engineering where the employees are unwitting participants. Often insiders are angry and want revenge, or are even paid to steal data, or wreak havoc.

Insiders should be subject to Least Privilege Access Policies to minimize damage. And IT should be able to track inappropriate sharing of data, and all end user actions to detect and prove malfeasance.

As much as cybercriminals around the world attack government systems, insiders can be a more insidious threat.

9. Failure to Log and Audit

Systems such as Office 365 collect literally millions of bits of information – for larger shops it takes little time at all to reach this many data points.

CoreView provides 1-year audit data collection, which can be extended however long the customer wants. However, ask yourself:

- Why do you need to collect these data logs?
- How does this impact regulatory regulations?
- What happens if you do not save and mine that audit data?
- What is the business impact?

How CoreView Exposes and Analyzes Logs

CoreView can produce a log in seconds for every end user or administrative action taken in Office 365 since the platform was initiated.

Real-time monitoring and alerts for security compliance issues is the engine that drives much of the data that forms the logs. Smart IT shops now enable real-time monitoring and alerts for potential security compliance issues in their Office 365 environment.

CoreView is Your Governmental Security Partner

Learn more about optimizing and securing Office 365 remote workers with a CoreView demo.

Get your O365 user workload usage and security profile FREE with our new CoreDiscovery solution. You can get your free software now at the CoreDiscovery sign up page: https://www.coreview.com/core-discovery-sign-up/

Doug Barney was the founding editor of Redmond Magazine, Redmond Channel Partner, Redmond Developer News and Virtualization Review. Doug also served as Executive Editor of Network World, Editor in Chief of AmigaWorld, and Editor in Chief of Network Computing.

Smart IT shops now enable real-time monitoring and alerts for potential security compliance issues in their Office 365 environment.