Building a better working world

How to protect your organization from ransomware

A layered defense strategy to reduce the risk of a ransomware attack

Successful ransomware attacks increased in 2019 and 2020, and that trend does not appear likely to end soon. EY teams have analyzed common ransomware attack patterns to help clients better prevent these damaging attacks.

There is no "silver bullet," product or solution that can fully protect an organization from ransomware. Nor is it possible to outline a broad cyber defense strategy in a single paper. However, EY teams can review specific areas that attackers typically target as part of their strategy. This paper aims to help identify controls or leading practices that, when implemented, can reduce the likelihood of a successful ransomware attack against your organization.

Contents

How to decrease a ransomware attacker's chances of accessing your network

Cybersecurity practitioners promote a multilayered (defense in depth) approach to prevent successful attacks. All agree that hardening the exterior shell is a necessary defense. Organizations must decrease the attack surface and make the organization a more difficult target to exploit. Consider these four areas of focus.

1. Protect against insider threats

Despite all efforts to secure the exterior threat surface, your work is not complete until you manage the most significant cyber risk to any business — the human factor. Not all insider threats are malicious. Employees are human and make mistakes, despite their best efforts and intentions. Bad actors often focus their efforts on phishing employees to obtain needed credentials or system access for an attack. This practice became more successful during the pandemic when attackers began preying on anxiety about COVID-19. To reduce the opportunity for successful phishing attacks, focus on training and testing individual employees.

- **Train employees.** Provide training annually, at a minimum, regarding computer usage, email usage, internet usage, data handling and disposal, cyber incident reporting and handling, and other safe practices. Implement regular security awareness campaigns at all levels of the business to embed security into your company's culture. This helps employees to automatically consider cybersecurity in every decision they make, which can help keep your organization safe.
- **Test employees.** Randomly test employees, at least quarterly, to determine if they are susceptible to phishing scams. Provide additional resources and training to employees who struggle. A phishing test allows organizations to send employees an email that looks real, but is completely fake to test their users.
- **Implement an email gateway.** Deploy and configure an email gateway to scan and block malicious email, including embedded links and attachments.
- **Implement URL filtering and blocking.** Reputational analysis and scoring can reduce the likelihood of success of many phishing attempts and prevent malicious clicks from delivering their payload or exploit code.
- **Implement sender policy framework (SPF).** Reduce the chance of spoofed emails by implementing SPF or domain-based message authentication, reporting and conformance (DMARC). Refer to CIS Control 7[1] for additional guidance.

[1] "Email and Web Browser Protections," *Center for Internet Security website*, https://www.cisecurity.org/controls/email-and-web-browser-protections/, accessed July 25, 2020.

- **Warn email recipients.** Tag external email with warning messages that it originates outside of the organization to give employees additional warning.
- **Empower email users.** Provide an easy process for employees to report suspected phishing emails to IT for investigation and confirmation.

There is no perfect network protection. Threat attack methods are constantly changing, as are the attack surfaces, and it is virtually impossible to consistently avoid infiltration. It is important that organizations assume an attacker will get past their best defenses. But fortunately, there are additional controls at the internal layer that can make life difficult for an attacker and even stop an attack.

An attacker's goal is to obtain persistence and escalate access privileges. Ransomware, by nature, is not self-propagating. Attackers require significant access and leverage to propagate ransomware across the IT environment. If attackers gain access to broad system administrative credentials, or worse yet, domain administrative credentials, they have generally achieved the pinnacle of enterprise intrusion.

With these credentials, attackers can use your infrastructure to widely disrupt IT systems, including leveraging active directory and group policy to deploy ransomware. Organizations should do everything they can to protect privileged accounts and administrative access within their environment. Without privilege, attackers are limited in their ability to widely impact the organization.

Specific vulnerabilities and threats are constantly being discovered. In addition to the recommendations provided, all organizations should consider a comprehensive threat intelligence plan to identify new threats as they appear.

Unfortunately, in our experience, many organizations make gaining privileged access too easy. The following three steps can significantly limit the ability for an attacker to gain administrative access rights.

2. Protect exposed systems and applications

Organizations should also look to protect externally exposed and vulnerable systems and applications. Systems exposed externally with open vulnerabilities make for an attractive and easily exploited target. Ransomware attacker groups continue to successfully target unpatched vulnerabilities applications and systems, including but not limited to Windows Shares (SMB) (CVE-2020-0796), PulseVPN (CVE-2019-11510), F5 Big IP (CVE-2020-5902), Palo Alto Global Protect (CVE-2020-2034) and Citrix NetScaler (CVE-2019-19781). Specific vulnerabilities and threats are constantly being discovered. In addition to the recommendations provided, all organizations should consider a comprehensive threat intelligence plan to identify new threats as they appear.

- **Secure configurations.** Establish, implement and manage a secure configuration for each system on the network. If you are unsure how to do this, the Center for Internet Security (CIS Control 5[2] can provide general guidance on leading practices.

[2] "Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers," *Center for Internet Security website*, https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/, accessed July 25, 2020.

- **Enforce access controls.** Regularly review access controls and confirm proper access on any publicly exposed applications or systems, including cloud storage units.
- **Scan systems for vulnerabilities.** At least quarterly, complete a vulnerability scan of all systems and applications, and remediate all high-severity vulnerabilities.
- **Patch systems.** Verify that you have a process in place to maintain current software and firmware levels on all exposed systems and applications (i.e., a patch management process). Many vulnerabilities remain open to attackers simply because organizations lack a systematic patch process.
- **Secure Windows SMB.** Never expose Windows SMB to the internet. Attackers can easily find and compromise Windows systems by deploying malware to systems on your internal network through exposed Windows SMB.

3. Implement advanced endpoint detection and response (EDR) solutions

Advanced EDR solutions use proactive techniques, such as machine learning and behavioral analysis, to identify potentially new or complex threats. EDR solutions can quickly identify an attack, its scope across your network, and isolate and/or quarantine infected systems to stop the attack. These advanced techniques make it much more difficult for an attacker to establish a solid footing on your network.

Whichever advanced EDR solution you chose, strongly consider deployment of this capability across all end points (e.g., end user systems, servers, IoT).

- **Deploy EDR:** Deploy EDR widely across endpoints on your network, with a focus on privileged user systems and infrastructure servers. Work with your chosen vendor to verify that your EDR solution is configured to take full advantage of its capabilities.

  Consider implementing an advanced security monitoring team that can respond to EDR alerts to investigate suspicious traffic and carry out proactive threat hunting for faster detection and remediation of threats. This team will help protect your organization's assets like data, business systems, operational technology and brand.

  Where it is not possible to use EDR (e.g., supervisory control and data acquisition [SCADA] systems and legacy systems), confirm the systems are isolated from the internet and completely segmented from the rest of your network. For operational technology (OT), use data-diodes where you need one-way communication, such as data or information retrieval from systems, devices and programmable logic controllers (PLCs), and more.

4. Secure your network services

One of the most common methods for initial access to an environment is the exploitation of insecure network services, especially remote desktop protocol (RDP). To reduce the risk of exposure from insecure network services, consider the following steps.

- **Disable unnecessary services.** Perform a comprehensive assessment of all exterior-facing systems, disable unnecessary services and monitor those that remain.
- **Integrate threat intelligence.** Leverage threat intelligence to prioritize prevention and detection efforts. Use intelligence from industry vendors to prioritize identification and patching of common vulnerabilities and exposures (CVEs). Implement leading-practice security configurations, enhance security operations center (SOC) detection capabilities and increase rigor in your internal and external testing assessments.

  Consider implementing a threat intelligence gateway (TIG). A TIG is a device that sits on the exterior of your network and is updated, sometimes hourly, with an intelligence feed that lists all the known malicious IP addresses and domains from which many attacks originate. It then blocks any traffic coming from or going to these known malicious sources — eliminating much of the attack traffic from ever affecting your network to begin with.

What happens if an attacker finds a way past my outer defenses?

- **Secure remote management services and RDP.** RDP was designed as a convenient method for managing Microsoft Windows servers remotely while on the same private network — it was not originally intended for use over the open internet. Often unsecured and overlooked by management, attackers seek to exploit RDP when it is externally exposed to the internet.

  If you use RDP, or any remote management service, configure it so that it sits behind a remote access gateway or a virtual private network (VPN), preferably with two-factor authentication implemented. Limit access to only those who need it and monitor for unusual access or behavior patterns.

If you are unable to place RDP behind a gateway:

- Limit access to only those who need to use it
- Implement strong authentication, ideally two-factor authentication
- Configure it to use network-level authentication, which requires users to authenticate before an RDP session is established
- Implement account lockouts to limit brute-force attacks
- Restrict access by implementing firewall rules that only allow RDP activity from a list of known and trusted IP addresses
- Implement endpoint detection and response on the RDP server and monitor all connections via a security information and event management (SIEM) solution to watch for potential abuse

1. Identify privileged accounts

You must know who can access what on your network. Inventory where administrative rights are available in your network and identify every employee who has administrative access. Dig deeply. It is easy for organizations to overlook administrative privileges on unique systems, network devices, IoT or other systems. It only takes one overlooked administrative credential set to default, or another form of weak password, for an attacker to exploit and gain the access they need.

- Inventory all systems on your network and identify all administrative or privileged accounts
- Identify who has access to each account and determine if they truly need that access to perform their job
- Identify the purpose of service accounts, as well as which services they run, what systems they access, and how often they access those systems
- Identify weak and common passwords shared across privileged user and service accounts and change to provide diversity and complexity

2. Implement a privileged account policy

Once you have identified all forms of administrative and privileged access in your environment and determined who is using that access, you need to define policy for your organization.

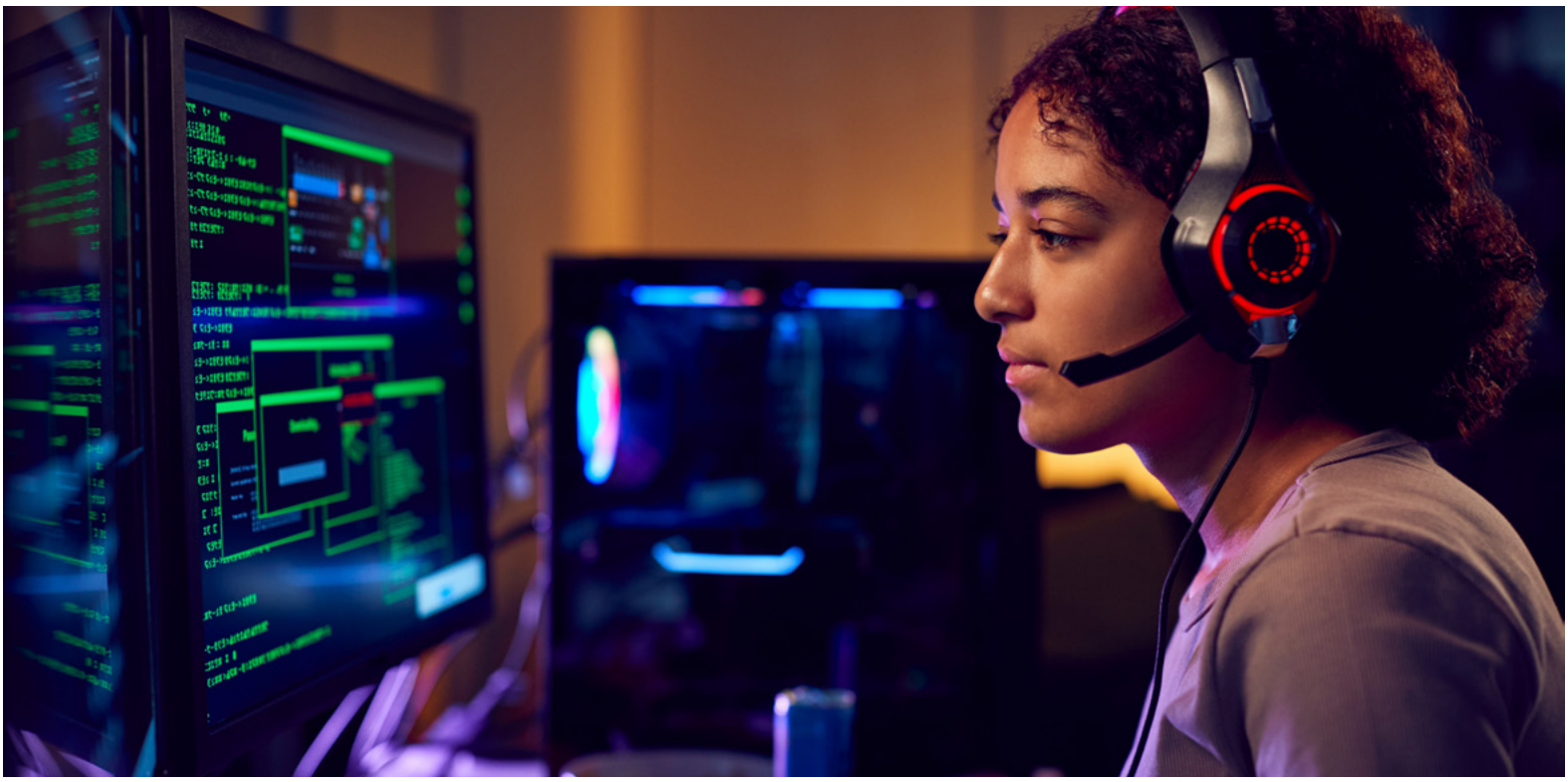
CIS Control 4[3] provides leading practices you can refer to when creating your policy. The following practices are critical to reducing the risk of an attacker compromising administrative access credentials.

- Implement requirements for unique and strong passwords for administrative access on each system, or limitations on where and how to use them.
- Restrict the number of people who have administrative or privileged access to those who need it to complete job responsibilities. A suggested method is to implement additional controls in your digital identity solution that identify administrative and privilege roles, enforce your defined policy and facilitate regular auditing for continued access. If you have a digital identity solution and have not done this, work with your vendor to configure and put this capability in place.
- Implement restricted access to end-user systems. Employees should not log into their standard workstation with administrative credentials. Further lock down these systems with a strong security policy, including restricting access to Registry Editor for Windows end-user systems.
- Verify that every ID with elevated privileges is unique and follows a strong password policy. Making the password the same for administrative access, on any system and all administrative IDs, across the enterprise may be convenient for your organization, but makes it easy for an attacker to wreak havoc across the enterprise once a privileged account is compromised.
- Service accounts are often overlooked. Confirm that all service accounts are configured to have the minimum privileges necessary to do the job they are intended to do. An overprivileged service account can be the means for an attacker to move laterally through the environment, despite implemented leading practices on other administrative or privileged accounts.

For privileged accounts across IT assets, applications and infrastructure, consider implementing a centralized Password Solution or Password Vault, which provides the ability to:

- Securely and centrally store privileged credentials and randomize passwords
- Develop an audit trail for privileged activity
- Provide user behaviour and threat analytics on privileged activity

[3] "Controlled Use of Administrative Privileges," *Center for Internet Security website*, https://www.cisecurity.org/controls/controlled-use-of-administrative-privileges/, accessed July 25, 2020.



- Automatically enforce standards and policies which govern privileged accounts
- Allow for the management and control of service accounts
- Abstract privileged account passwords from end users through session management capability
- Implement multifactor authentication (MFA) for all privileged and administrative access accounts. If attackers compromise an administrative account password, operationalized MFA would make it very difficult, if not impossible, for them to take advantage of it.
- Do not allow those who have administrative access to authenticate to their employee workstation with elevated privileges. Every employee, including IT staff, should be provisioned a standard user access account with restricted or least privileges on their normal workstation. In other words, employees should only be given appropriate user access that allows them to complete tasks on their workstations that are necessary for their job. Employees should not be allowed to log in with administrative access to their workstation as part of day-to-day normal activity or process.

- Restrict those with administrative privileges to use it only when necessary to complete a task that requires elevated privileges. Ideally, implement a privilege access management (PAM) solution, which requires an employee to request the necessary escalated privileges, be approved for the access and then be enabled to complete the work for a certain period of time. PAM solutions can be very effective in minimizing the ability for an attacker to stumble across an employee logged in with elevated privileges and compromise those credentials.
- If you do not currently have a PAM capability in place, consider restricting administrative access and tasks to only be completed on a jump server or privileged access workstation (PAW). A PAW is a designated workstation that is isolated from the internet, securely configured and restricted from many user features, such as external email, and is designated as an operational hub for administrative access. Do not leave administrative accounts logged in on a workstation continuously on any system.
- Do not use easy-to-identify descriptors for privileged accounts. Many organizations use a common identifier such as "ADM" to identify administrative accounts, e.g., "adm-joe01." While convenient and easy to use, it makes it easy for attackers to identify privileged accounts when scouting out the environment. They can then focus their compromise efforts, including password cracking and administrative user workstation compromise, on those accounts.

3. Monitor your environment for unusual privileged user behavior patterns

Once your privileged access is protected, monitor it for anomalous behavior. This is especially critical not only to detect and prevent a ransomware attack but also other significant cyber attacks as well.

- If you are using a PAM solution for privileged access, you may have a capability to monitor use of privilege and identify anomalous behavior patterns. Even if you are fully leveraging your PAM monitoring and detection capabilities, consider contacting your vendor to identify other ways you can monitor privileged access use.
- There are solutions and vendors that can perform in-depth monitoring of anomalous behavior patterns for various systems in your environment. EDR is one example. Review the controls you currently have in place that identify unusual behavior and consider where you may have gaps. Refer to CIS Control 6[4] for further leading practices in this area.

  Strong management of privileged and administrative access can be one of the most effective ways to limit the ability of an attacker to harvest data or launch a ransomware attack in your environment.

[4] "Maintenance, Monitoring, and Analysis of Audit Logs," *Center for Internet Security website*, https://www.cisecurity.org/controls/maintenance-monitoring-and-analysis-of-audit-logs/, accessed July 25, 2020.

I've been infected with ransomware. What now?

Even when following all leading practices, there is no guarantee your organization will never be affected by a ransomware attack. Organizations should develop the appropriate level of organizational resiliency and redundancy that will limit damages and allow for a quick recovery from a disruption event. The following items can help establish organizational resiliency after a ransomware event.

Backup and secure your critical data

Verify that you have a process in place to securely back up all your critical data. Unfortunately, in many ransomware events, the attacker may have disabled, deleted or encrypted your backups. If ransomware has encrypted your data, it is likely there is no publicly available decryption key, and you are faced with the decision to pay a large ransom demand to obtain a decryption key. Recent enforcement action taken by the Office of Foreign Assets Control within the U.S. Department of Treasury may limit your organization's ability to pay ransom demands to certain ransomware groups.

- Implement a secure backup process that involves multiple copies, some of which are offline and protected. You can utilize traditional tape backups with off-site storage service, cloud-based solutions or other methods. In every case, confirm that your backups have restricted access and are secured. Confining your data backups to a single system connected to your network is a big risk that allows the attacker to inhibit your ability to recover.
- Continually test your organizational ability to recover in a timely fashion from your backups. At least twice a year, test your ability to recover different critical systems and data. Unfortunately, many organizations learn during a ransomware event that what they thought was a robust system of backing up their data is either too slow or they are unable to use them to recover at all.

Refer to CIS Control 10[5] for additional information on leading practices in defining and testing your data backup and recovery process.

---

[5] "Data Recovery Capability," *Center for Internet Security website*, https://www.cisecurity.org/controls/data-recovery-capability/, accessed July 25, 2020.

Create a response plan

Every organization should have a cybersecurity incident response plan in place. When your organization has a defined plan — and has practiced it repeatedly — you are more likely to avoid the panic and delayed reactions that can exacerbate a ransomware event and increase damage and costs.

- When creating your organization's cybersecurity incident response (IR) plan, verify that your plan includes all roles involved in your response — internal and external — that may be involved, including key support contacts and vendors. The plan should define the responsibilities for each role and the general steps that must be taken to identify, contain, remediate and recover from a cybersecurity incident.
- Consider the role of external providers and resources in your IR plan. In addition to third-party IT vendors, you may need assistance from vendors who specialize in cybersecurity and forensics, cyber legal counsel, as well as communications and public relations. You can often establish a relationship with these firms before a ransomware event via a retainer, which establishes contractual terms, pre-negotiated rates and proactive capabilities that enhance your ability to respond to a cyber incident. Once you have an organization identified and a retainer in place, add that firm and contacts to your incident response plan.
- Test your response plan. This is typically done through tabletop exercises, where all required personnel can simulate, in a safe way, an actual ransomware event. This helps confirm that tools, processes, methods and people are prepared. The more an organization practices, the more it will identify ways to improve the plan, train its people and reduce panic when an event occurs.

Refer to CIS Control 19[6] for more information on leading practices to define and test your data backup and recovery process.

---

[6] "Incident Response and Management," *Center for Internet Security website*, https://www.cisecurity.org/controls/incident-response-and-management/, accessed July 25, 2020.

How EY teams can help

Ransomware can be costly and damaging, and it continues to become more sophisticated. Organizations should actively keep abreast of the latest attack patterns, address vulnerabilities and update response plans.

EY Cybersecurity Consulting can assist you to with your ransomware risk management strategy with customized approaches for your organization, including:

- Cyber threat intelligence
- Cyber risk management and planning
- Business resiliency
- Identity and access management
- Privileged access management
- Detecting and responding to active threats
- Incident response planning exercises

Contact us for more information on protecting your organization from ransomware.

Yogen Appalraju
EY Canada Cybersecurity Leader
yogen.appalraju@ca.ey.com
416 932 5902

Chandra Majumdar
EY Canada Cyber Threat Management Leader
chandra.majumdar@ca.ey.com
416 941 1833

Omer Arshed
EY Canada Digital Identity Co-Leader
omer.arshed@ca.ey.com
416 943 3800

Keith Mularski
EY Americas Cyber Threat Intelligence Leader
keith.mularski@ey.com
412 644 0612

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

3749339
ED None

ey.com/ca