One of the most visible results of the 2020 COVID-19 pandemic has been the mainstream transition from traditional office-based work to remote work-at-home arrangements. Government officials worldwide mandated that nonessential employees stay home. Enterprise leaders followed the government mandates by directing employees to isolate at home to keep the virus from spreading throughout employee populations. A primary lesson from that experience is that employees and the critical functions they perform can be protected and maintained by initiating secure remote teleworking operations. Unfortunately, as figure 1 depicts, remote working introduces new IT-related threats that require unique threat mitigation countermeasures.

These countermeasures can be organized under five categories:

1. Employee security
2. Endpoint security

<table>
<thead>
<tr>
<th>Figure 1—Remote Work Threats and Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat</strong></td>
</tr>
<tr>
<td>Theft of teleworking endpoints and devices</td>
</tr>
<tr>
<td>Unauthorized monitoring, collection or modification of traffic passing over teleworking networks</td>
</tr>
<tr>
<td>Telecommuting-specific increases in endpoint malware infection</td>
</tr>
<tr>
<td>Pandemic-specific phishing attacks</td>
</tr>
<tr>
<td>Pandemic-specific malicious website infections</td>
</tr>
<tr>
<td>Remote teleworker outages and service request management</td>
</tr>
<tr>
<td>Theft or destruction of enterprise intellectual property by temporarily furloughed or laid-off employees</td>
</tr>
</tbody>
</table>

**Brett Bonin, CISA**

Is a successful cybersecurity executive with extensive experience leading world-class corporate security transformation and optimization programs. Bonin currently directs global security strategy and operations as the deputy chief information security officer of Omnicom Group, a Fortune 100 international marketing company with five major subsidiary networks: DAS Group of Companies, DDB, BBDO, Omnicom Media Group and TBWA. He leads the organization in securing both corporate IT and the intellectual property of more than 5,000 business clients in more than 100 countries, including brands such as Apple, AT&T, Cisco, Hewlett Packard, Microsoft, Nike, PepsiCo and the US Army. Bonin honed his security and business leadership practices through 25 years of mentoring from the best global executive leaders, and he has diverse senior-level experiences in private- and public-sector roles. He is a retired US military officer with 25 years of decorated service in cyber, engineering and intelligence.
3. Network security
4. Security monitoring
5. Security reporting

Each of these categories contains security areas that, if ignored, could result in serious risk both during the transition and longer term operational approach to predominantly working remotely. Enterprise leaders should evaluate each one for applicability to their unique environments.

Employee Security

Employee security is one of the five categories that require unique countermeasures. Employees are often the weakest link in enterprise security because they have countless opportunities to make decisions that could lead to a security breach. Employee security focal points include teleworking policy, training, antiphishing, and identity and access management (IAM):

- **Teleworking policy**—A solid work-from-home policy that accounts for pandemic-related threats is an essential starting point for maintaining safe and continuous business and IT operations. The work-from-home policy should specify what enterprise leaders expect from employees who are working remotely. It should emphasize cybersecurity considerations, such as safe remote computing, acceptable use and sanctioned applications. Acceptable use is a general concept that may have been in effect before the pandemic, so enterprises should create an exception to policy and procedure to enable users with special-case scenarios to perform functions that would otherwise be restricted as unacceptable. The policy should provide information such as who to contact in the case of lost or stolen devices, phishing, or the observation of suspicious computing events. The teleworking policy should also intersect with enterprise training and provide a list of mandatory training courses aimed at mitigating the threats specific to telecommuting. Critical to a safe remote work environment is the virtual private network (VPN) that provides connectivity from home offices to enterprise systems. Remote workers should have access to all the how-to information they need to connect remotely over the VPN.

- **Employee training**—Training managers should consider creating specialized training content to empower employees with the knowledge to manage the unique threats they will face while teleworking. Training should include policies governing work-from-home computing rules and tutorials that prepare end users for potential threats, such as laptop thieves or pandemic-specific phishing emails.

- **Email antiphishing services**—Enterprise leaders should prepare for new pandemic-specific phishing tactics. For example, hackers may send malicious emails to employees under the guise of pandemic-related subjects to make them seem more relevant and to trigger an emotional impulse to click on the malicious link or file attachment. The enterprise should implement or fine-tune antiphishing platforms to account for messages with pandemic signatures coming from external sources.

- **IAM**—IAM teams need to both grant new access and remove existing access based on unique pandemic-specific considerations. Onboarding and offboarding employees remotely will require IAM actions to create, temporarily disable and delete employee IAM credentials and underlying authorizations. Multifactor authentication (MFA) is also imperative, particularly for anyone connecting from remote locations to perform elevated administrator and high-risk functions. Certain industries and job functions that involve sensitive data should ensure that all systems that store, process and transmit sensitive data are hardened through enhanced IAM security measures such as centralized log correlation,
monitoring and retention of user login attempts and access. MFA is wise for users performing job functions involving high-risk sensitive data.

**Endpoint Security**

The endpoint security category is the second of five categories that require unique countermeasures. Weaknesses in endpoint and device security can provide an abundance of opportunities for threat actors to gain unauthorized access and damage the integrity and availability of data. Endpoint and device security focus areas include endpoint encryption, endpoint management services, antivirus services, endpoint vulnerability and patch management, backup and restore, web content filtering, application security, and cloud access security broker (CASB):

- **Endpoint encryption**—With so many employees working remotely, many more laptops will be used outside the office in remote locations without physical security protection. By directing the encryption of endpoint hard drives and sensitive files, enterprise leaders can be assured that laptop and mobile device thieves will not be able to access data.

- **Endpoint management services**—Managing laptops and devices remotely over the Internet is more important when the majority of employees are teleworking. For example, existing patching platforms may double as mobile device management (MDM) platforms. Windows System Center Configuration Manager (SCCM) and Apple Jamf have remote wiping and locking capabilities that IT and security leaders can use to maintain the confidentiality of data, intellectual property and trade secrets. These platforms can also be used to partition and ultimately wipe, if necessary, enterprise data without impacting personal data on personal mobile devices if the enterprise has a bring-your-own-device (BYOD) program.

- **Antivirus services**—Next-generation antivirus services inhibit the execution of malicious logic on endpoints, servers and devices. These types of preventive security tools do not rely on static malware signatures alone, but block the execution of malicious logic based on artificial intelligence (AI) and machine learning to protect against zero-day exploits. Next-generation antivirus services provide better protection than legacy signature-based services.

- **Endpoint vulnerability and patch management**—More remote teleworking translates into more scanning and patching and greater exposure to threats. Remote workers connecting to insecure home and public networks, particularly those bypassing centralized enterprise IT security services, are much more vulnerable than typical in-office workers. Patching endpoint vulnerabilities is part of basic computing hygiene that becomes more important during teleworking.

- **Backup and restore**—The ability to restore data from backup is essential to any operating environment exposed to threats that can alter the integrity and availability of enterprise data. If user data are backed up, enterprise leaders can mitigate threats such as ransomware viruses and stolen laptops and other devices by ensuring that lost data can be recovered and restored.

- **Web content filtering**—Hackers may create malicious pandemic-related websites containing malware that could compromise remote user endpoints and, ultimately, allow hackers to enter the enterprise network or steal data from the end user. Content filtering services can be tuned to filter out malicious pandemic content.

- **Application security**—Employees may use their enterprise endpoints to access consumer cloud applications (e.g., messaging, video) that can expose the enterprise to significant risk. Enterprise IT leaders should identify and patch these third-party applications or remove them from employee endpoints.
Cloud access security broker (CASB)—CASB services can provide enterprise leaders with insight into what types of applications employees are using and what types of data they are uploading and downloading. The CASB also allows the enterprise to control risky cloud activities.

Network Security

Network security is the third out of the five overall categories that require unique countermeasures. A network is the “highway in” and should be both resilient and robust while also serving as a “checkpoint” into restricted areas with restricted data. Network security countermeasures include high-availability remote access infrastructure, network access control (NAC) and enhanced technical support:

Hardened high-availability remote access infrastructure—With a shift to remote teleworking, VPN system security and resilience become more important. Without hardened, strong encryption, attackers can exploit weaknesses in remote connectivity systems to either gain unauthorized system access or collect and/or modify data in transit. Network staff can harden VPN systems by requiring MFA to augment the simple stand-alone username and password, making it much more difficult to exploit and gain access. Scanning for VPN infrastructure vulnerabilities and then patching and configuring them to a hardened and secure state are critical when work is performed remotely over VPNs. The VPN system should be resilient and implemented in a redundant, high-availability architecture to ensure that there are no single points of failure. The network team must also provision the VPN to support large increases in remote user traffic, making centralized Internet capacity and circuit redundancy more critical as well.

Network access control (NAC)—NAC services perform a gatekeeper function by not allowing users and their laptops or devices to connect to enterprise services without passing system checks. NAC systems also provide an actionable compliance status for each endpoint based on a set of enterprise security policy requirements. Managers can designate which segments and resources VPN-connected users can access in accordance with the principle of least privilege based on compliance status and employee identity. Security leaders can effectively cordon off endpoints that might be susceptible to threats based on the NAC system-generated risk profile for each endpoint prior to connecting to the network.

Enhanced technical support—Technical support processes, which would typically include physically bringing laptops and other devices to work for repair and inspection, need to be updated to conform to constrained pandemic operations when only remote access is feasible. Technical support teams will require secure remote desktop applications. IT leaders should evaluate all remote management applications and ensure that staffers harden them to the fullest.

Security Monitoring

Security monitoring is the fourth out of five overall categories that require unique countermeasures. Every node on the network produces event logs that security professionals can leverage when piecing together clues during an investigation. Security practitioners can deploy security information and event management (SIEM) platforms to centrally correlate and store event logs for future analysis during investigations. A shift to remote teleworking involves specific systems that produce unique logs that need to be a new focus.

SIEM includes central correlation and monitoring of events from security platforms that indicate
potential compromise from pandemic-related threats. The monitoring team should ensure that specific events from the following types of sources are being monitored for malicious activity:

- Security system availability
- Endpoint malware infections
- VPN
- Identity and access authentication requests and failures
- MDM
- Email antiphishing services

Enterprise security leaders should consider creating specialized reporting capabilities that provide the status of security services aimed at mitigating pandemic-related threats. The following are examples of specialized reporting:

- Number, type, purpose and criticality of remote user endpoints not reachable by endpoint management systems such as patching, antivirus, MDM and encryption
- Access logging and monitoring of privileged administrative access to high-risk systems and functions
- Employee and system compliance reports with current vulnerabilities, prioritized by the most critical vulnerabilities
- VPN-specific indicators and metrics, such as availability, employee logins and data specifics
- Remote user backup status
- CASB reports on risky remote user cloud data transfers and risky public cloud application use
- Remote worker policy exceptions
- Remote worker acceptable Internet usage

Conclusion

When pandemics such as the COVID-19 outbreak lead to a widespread, rapid shift to remote working in home offices, the enterprise threat landscape changes, and enterprise IT security leaders must deploy specific enhanced threat mitigation countermeasures. By implementing enhanced IT security countermeasures in employee security, endpoint security, network security, monitoring and reporting, enterprises can ensure that business systems will continue to operate in an unimpeded, secure manner.

Enjoying this article?

- Learn more about, discuss and collaborate on risk management in ISACA’s Online Forums. https://engage.isaca.org/onlineforums