Incident Response During the Global COVID-19 Crisis

Since March 2020, the global COVID-19 pandemic has affected the characteristics of incident response (IR) in the cybersphere. These unprecedented times have forced some enterprises to deal with their most severe business crises to date and to cope with the pandemic's impact on the threat landscape. For incident response practitioners, COVID-19 has been a significant factor in planning and execution in almost every engagement. Alongside the physical aspect of working remotely, there were other direct and partially direct aspects, such as technical remote access issues or the client's available funds and human resources. However, despite the challenges, as the market and organizations have adjusted further, business and technological opportunities have been created.

OFIR EITAN | CISM, CDPSE, CCSK

Is a digital forensics and incident response (DFIR) manager with more than 15 years of experience in information security, primarily in cyberthreat intelligence, cybersecurity operations and incident response. Prior to this role, he spent five years working in finance in Israel and the United States. Prior to that, he served for 10 years in the Israel National Cyber Bureau and the Israel Defense Forces Intelligence Directorate as an information security officer. He can be reached at *www.linkedin.com/in/ofir-eitan*.

Remote Work

For providers of professional services, the COVID-19 pandemic has created new business opportunities, both domestically and globally. New markets became accessible when the traditional method of sending workers onsite was no longer feasible and enterprises were required to adapt and learn to operate remotely. After a rough start for some, enterprises from all sectors have adjusted to the new norm, and IR organizations have done so as well.

IR professionals have streamlined processes, focusing on what is important, avoiding background noise and neutralizing other factors that can typically distract parties during an onsite incident management process. Most notably, some IR professionals have noticed that meetings that used to take between 90 and 120 minutes are now lasting no longer than an hour, and the results are the same, if not better.

On a tactical level, incident responders have learned to execute digital forensics data collection and run detection rules remotely, with no hiccups or bottlenecks. Legacy systems or isolated networks are sometimes encountered, but IR teams have developed processes and services to overcome such problems. If necessary, incident responders or liaisons can be sent onsite for specific assignments, but this has become the exception rather than the rule. This makes the service more cost-effective for clients because it allows the service provider to use fewer human resources. Instead of sending a task force consisting of an executive, an incident responder, a threat intelligence officer and an IT specialist with remote support from the rest of the IR team, the service provider can use few or even no onsite resources. Besides the immediate value accruing for both the client and the service provider, the past two years have also been valuable for educating the market on how to operate remotely, which prepares the market for future crises such as environmental disasters, conflicts or domestic unrest.

Personnel Management

During the pandemic, incident response has taken a sharp turn in terms of group dynamics and business decision-making. Traditionally, in an enterprise office environment, managing an incident is composed of two primary elements: board meetings and working teams. However, huddles in much smaller groups may also take place throughout the day when teams are facing significant milestones.

Board meetings usually take on the characteristics of a war room, with every primary function presenting its status and next steps. Occasionally, whenever key individuals are not present (for any number of reasons such as geographic distance, flight delays, traffic), their absence can directly impact the making or execution of decisions. Imagine trying to recover from a fatal ransomware attack or run the decryptor after making a ransom payment if key IT figures have yet to arrive on premises. Remote IR services solve almost all these issues and even created new opportunities, including creating the opportunity for the IR enterprise to reallocate resources and assign professionals to multiple cases, especially if they are located in another region or country. In remote IR engagement, all gatherings are funneled to virtual conferences that can be taken from anywhere with minimal roadblocks, even if multiple parties are geographically located far away. For example, if the IR task force used to be dispersed between different previous client sites, while working remotely, the team can easily gather for a preparation call and join the kick-off call with the client within a matter of hours. Working remotely has solved a majority of the physical roadblocks and coordination issues that existed. A similar process applies to other parties involved in the incident in addition to the client, such as the breach counsel, insurance carriers, other third-party vendors and, in some cases, government entities (e.g., a community emergency response team [CERT]).

Patch Management

Patch management to mitigate exploited vulnerabilities, such as zero day, one-day or disclosed flaws, is one of the most challenging security controls to implement. Large enterprises are challenged by typically needing to handle high volumes of system inventory, while small enterprises are challenged by typically having fewer human resources to perform this function. Information security professionals typically agree that, when faced with a limited budget, organizations should hold off on investments, and in times of uncertainty, such as the COVID-19 pandemic, they should stick to the basics. Patching is a fundamental information security control that mitigates some of the most severe threat scenarios, including ransomware attacks and data breaches. Unfortunately, many enterprises of all sizes still do not follow this approach, and they have been compromised due to inadequate network hygiene. For instance, deep into the third and fourth quarters of 2021, some enterprises with unpatched Microsoft Exchange servers were still dealing with the effects of ransomware attacks caused by the ProxyShell vulnerabilities, first disclosed in March 2021.[1] Crises can sometimes offer opportunities, such as pausing to review current processes and improve them. Unfortunately, some enterprises are still struggling with patch management, and it seems that many did not take advantage of the COVID-19 restrictions to revamp their process.

"During the pandemic, incident response has taken a sharp turn in terms of group dynamics and business decision-making."

To improve patch management, there are three core elements that should be implemented. First, the organization should have an approved and documented process that addresses tasks, responsibilities and time execution regarding vulnerability discovery and remediation actions. This process should be based on a scoring method (e.g., Common Vulnerability Scoring System [CVSS]) to define prioritization and service-level agreements (SLAs). Second, the information security team should have a monitoring process to identify gaps in the network environment and address them in a timely manner, including exceptions. Exceptions can include expediting remediations due to high-criticality vulnerabilities (driven by intelligence or severity) or consulting on workarounds when patching is unavailable or unfeasible. Third, it is recommended the organization be equipped with a vulnerability scanner solution and supporting systems, designed specifically to address patch management process.

"Since the pandemic began, threat actors have capitalized on the ability to compromise only a handful of systems to gain access to multiple users and endpoints."

Evolution of the Threat Landscape

The control environment has changed substantially since the expansion of the work-from-home transformation. One immediate ramification was an exponential surge in security gaps. Working remotely generated new single points of failure, such as remote access platforms and videoconferencing applications.

Since the pandemic began, threat actors have capitalized on the ability to compromise only a handful of systems to gain access to multiple users and endpoints. In addition to the common tactic of compromising the vulnerable Remote Desktop Protocol (RDP), ransomware groups have exploited vulnerabilities in virtual private network (VPN) solutions. Some of the most notable common vulnerabilities and exposures (CVEs) include:

- Vulnerabilities in Citrix Application Delivery Controller and Citrix Gateway Directory (CVE-2019-19781), which was patched weeks before COVID-19 emerged but has been successfully exploited by ransomware threat actors[2]
- Vulnerability in Fortigate VPN servers (CVE-2018-13379), which was patched in 2019, but reused by threat actors since the pandemic began[3]
- Structured Query Language (SQL) injection vulnerability used to compromise the Colonial Pipeline's VPN system (CVE-2021-20016)[4]
- EntroLink VPN zero-day, discovered in September 2021 and used by ransomware threat actors[5]

Phishing attacks have used pandemic-related themes to lure victims. In 2020, threat actors aligned their phishing schemes with the pandemic's stage of development. From local restrictions to COVID-19 health advisories to vaccination instructions, whatever the center of attention, threat actors were able to cash in on attacks.[6, 7] Furthermore, there has been a surge in business email compromise (BEC) attacks, and the new remote work model has been a significant factor in this trend.[8] Naturally, it is more difficult to validate whether a suspicious email came from a coworker or manager if there is no chance of meeting that person in the elevator or in the break room while grabbing a cup of coffee.

Conclusion

For organizations in all sectors, the COVID-19 pandemic led to several challenges. Under budgetary constraints, unknown futures and adjustments to the new normal, organizations had to focus on adapting their basic information security practices to protect against new developing threats. There was also a rise in phishing schemes and exploited vulnerabilities in remote access solutions.

However, the COVID-19 pandemic's effects on the global market created more opportunities than challenges for IR service providers. The biggest change was the technological and cultural ability of enterprises from all industries to consume remote cybersecurity services. Organizations that continue to develop their remote capabilities rather than regress to past practices will be able to avail themselves of a wide range of cost-effective professional cybersecurity services with minimal limitations.

LOOKING FOR MORE?

- Read *Security Incident Management Audit Program.* *www.isaca.org/security-incident-management-audit-program*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Endnotes

1 Hope, A.; "LockFile Ransomware Attacks Exploit ProxyShell Vulnerabilities on Unpatched Microsoft Exchange Servers," *CPO Magazine*, 2 September 2021, *https://www.cpomagazine.com/cyber-security/lockfile-ransomware-attacks-exploit-proxyshell-vulnerabilities-on-unpatched-microsoft-exchange-servers/*

2 Nichols, S.; "CISA Unveils List of Most Targeted Vulnerabilities in 2020," *TechTarget*, 28 July 2021, *https://www.techtarget.com/searchsecurity/news/252504601/CISA-unveils-list-of-most-targeted-vulnerabilities-in-2020*

3 *Ibid.*

4 Jones, D.; "Colonial CEO Says Ransomware Hackers Exploited Legacy VPN," Cybersecurity Dive, 9 June 2021, *https://www.cybersecuritydive.com/news/colonial-Joseph-Blount-ransomware-legacy-vpn/601523/*

5 Cimpanu, C.; "Ransomware Gangs Are Abusing a Zero-Day in EntroLink VPN Appliances," The Record by Recorded Future, 25 October 2021, *https://therecord.media/ransomware-gangs-*

are-abusing-a-zero-day-in-entrolink-vpn-appliances/#:~:text=Multiple%20ransomware%20gangs%20have%20weaponized,the%20start%20of%20September%202021.&text=EntroLink%2C%20the%20South%20Korean%20networking,release%20by%20the%20security%20researcher.

6 Trend Micro, "Developing Story: COVID-19 Used in Malicious Campaigns," 11 November 2020, *https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains#:~:text=Trend%20Micro%20Research%20found%20coronavirus,as%20early%20as%20February%202020.&text=Now%20there%20are%20ongoing%20business,the%20disease%20as%20a%20hook*

7 Check Point, "Check Point Research: COVID-19 Pandemic Drives Criminal and Political Cyber-Attacks Across Networks, Cloud and Mobile in H1 2020," 21 July 2020, *https://www.checkpoint.com/press/2020/check-point-research-covid-19-pandemic-drives-criminal-and-political-cyber-attacks-across-networks-cloud-and-mobile-in-h1-2020/#*

8 Business Wire, "Abnormal Security Quarterly BEC Report Shows How COVID-19 Zeitgeist Permeates Email Cyberattacks on Businesses," Abnormal Security, 19 August 2020, *https://www.businesswire.com/news/home/20200819005457/en/Abnormal-Security-Quarterly-BEC-Report-Shows-How-COVID-19-Zeitgeist-Permeates-Email-Cyberattacks-on-Businesses*