EY Cyber Response To COVID-19

How to strengthen operational resilience and security during the COVID19 Crisis

The spread of Coronavirus could impact more than 5 million businesses worldwide[1]. In total, the most-affected countries represent nearly 40 percent of the global economy[2].

Enterprises across sectors face an evolving cyber threat landscape due to impacts from the pandemic.

- Furthermore a rapid transition to remote work puts pressure on security teams to understand and address a wave of potential security risks.

Recent cyber threats and attacks

Phishing, malicious sites, & business email compromise

- ► Cyber-criminals are exploiting interest in the global epidemic to spread malicious activity through several spam campaigns relating to the outbreak of the virus

Extortion or information theft & brand damage

- ► May target organizations perceived as under pandemic-related pressure
- ► Actions or statements considered inappropriate could trigger “hacktivism” and insider threats

Business Disruption from attacks

- ► “Coronavirus-themed ransomware” which can encrypt a computer's hard drive and let hackers demand payment to unlock it, has also been used

Dispersal of previously in-person activities and processes

- ► Change in network baseline:
  - Remotely performed high-privilege actions could trigger alarms
  - All traffic will appear anomalous until new baseline is established
- ► Increased load on help desk & IT

“ 79% Board members state that their organizations are not very well prepared to deal with a crisis event. [3]

Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak

ZDNet

Coronavirus-themed domains 50% more likely to be malicious than other domains

CheckPoint

Forbes

Coronavirus Scam Alert: Watch Out For These Risky COVID-19 Websites And Emails

RedDrip Team

Attacks pretend to be from the Center for Public Health of the Ministry of Health of Ukraine and deliver bait document

1Source: CNBC, 4February; 2Source: McKinsey, 3Source: Global Risk Survey 2020

The following actions could be considered to help protect your organization during this rapidly changing environment and recent cyber threats landscape.

Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations.

Pay better attention on the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery.

Implement Multi Factor Authentication (MFA) on all VPN connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords.

White listing and marking external emails. Furthermore, Inform employees about an expected increase in phishing attempts with Corona related topics and ask to don't click unknown suspicious links.

Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications—such as rate limiting—to prioritize users that will require higher bandwidths.

Web and email protection by implementing web filtering technologies to prevent employees from visiting malicious websites. Implement e-mail filtering rules to block spam and phishing e-mails. If you are a hospital or have a critical structure, you need to be stricter and consider whitelisting.

Closely monitor privileged access by optimizing the behavioral analytics tools for detecting suspicious activity for admins and those who handle critical data.

Limit administrator access and activities to the strictly necessary. Adm activities should also be better monitored and controlled (for example with a Four Eyes Principle).

Security Information and Event Management (SIEM) systems should be adapted, strengthening the log monitoring rules to trigger an alert. Security Operation Center (SOC) and monitoring teams should be available to manage the increased number of alerts, sorting them by risk, based on a strong process and detecting false-positives from real suspicious events.
For that, consider Staff increase.

Increase emergency management capacities, by reallocating resources. Check if your backup is working, test your failover capabilities . Help Desk should also be prepared to handle an increased number of events and the procedure to categorize those events

Increase your Endpoint monitoring protection

prepare for the worst, check crisis management and incident response capabilities internally and also availability of your providers. Maybe extend your provider landscape

What messages should be passed for your employees

1. Consistently follow your company policies
    - Policy, guidelines and rules for accessing the company network outside the office. Make sure to report any suspicious behavior to Support and follow basic standards: for example: keep an up-to-date operating systems, antivirus and malware, regular scanning, etc.
1. Don't allow family members to use your work devices
    - Treat your laptop, mobile device and sensitive data as if you were in your office location
2. Use your company approved storage solution
    - Make sure to store all your work data in a secure location that are approved by and accessible to your company.
3. Only use company-approved device and consult your IT department if you will be using a personal device to connect to corporate networks
    - If connecting through your home Wi-Fi ensure that they have a strong password and avoid using public or unsecured networks.
    - If a personal devise must be used, on an exception basis, be even more careful updating operating systems, antivirus, update FritzBox Router, etc.
5. Be mindful of your online hygiene
    - Be careful of clicking on suspicious links, especially if related to coronavirus, seeing that attackers are using that fear will better prompt victims to click without thinking.

Your EY Team

Petr Plecháček
Cybersecurity
+420 225 335 548
petr.plechacek@cz.ey.com

Petr Fojtů
Cybersecurity Manager
+420 225 335 449
petr.fojtu@cz.ey.com

Petr Brabec
Associated Partner
+420 225 335 743
petr.brabec@cz.ey.com

Petr Čivrný
Advisory Senior Manager
+420 225 335 168
petr.civrny@cz.ey.com