CYBER SECURITY GUIDANCE RELATED TO COVID-19

April 1, 2020
Version 1.0

TABLE OF CONTENTS

ABOUT THIS DOCUMENT

This guidance has been written to support ongoing efforts to help mitigate the changing cyber security challenges related to the COVID-19 pandemic. This document is created on a best-effort basis, and it is aimed to provide high-level advice to organizations in order to limit the impact of potential incidents as a result of the changing ways of working and new cyber security risks and threats related to them.

Finally, as also outlined in this document, all recommendations should be first evaluated in terms of feasibility and taking into account the increased workload of the IT operations teams. Only those suggestions should be implemented which can be properly tested and confirmed.

1. F-SECURE'S OBSERVATIONS RELATED TO THE CHANGING THREATS

1.1. Phishing

Attackers have already started exploiting the burst of information and heightened alertness of the public for COVID-19 related news. Phishing and spam campaigns and malicious websites/domains have significantly increased[1,2] in number and frequency in the past week, promising COVID-19 related information and guidance. This threat is further increased by the fact that a largely remote workforce comprised of people who are used to the easy access to colleagues to verify suspicious emails might be less likely to investigate such messages over online communication channels.

1.2. Ad-hoc infrastructure changes

As employees shift to remote work, most organizations are seeing heavy load on resources such as virtualized desktop environments and VPNs. The demand for seamless connectivity often wins over security. In order to facilitate a distraction free workflow, one might be tempted to let users access internal resources from untrusted networks, such as the Internet and personal devices. If these resources rely on the more trusted, internal network as their security model, this approach opens up a variety of risks to the organization ranging from unpatched software to lax authentication and authorization models for an untrusted network.

1.3. Changes to regular security-critical processes

Because the capacity of IT operations teams are limited and their normal workflows may be currently interrupted, some processes might see delays or postponements. One example that seems to be a trend is delayed patch cycles. To limit attacks that target known vulnerabilities, it is important to keep the time of patch cycles to the minimum following the release of a vendor security update even in this ongoing pandemic.

1.4. Insecure home networks

Each employee working from home, especially ones using their own personal hardware to access company resources expose a new untrusted network to the organization. As home networks are mainly comprised of commercial off-the-shelf hardware (COTS), they might not have the same security maturity as company-approved, corporate devices. This exposes several risks to the organization, mainly stemming from insecure IoT devices, which can be easy targets for both targeted and opportunistic attacks, and even for drive-by malware, such as IoT botnets, to which access is sold on black markets.

[1] https://www.zdnet.com/article/thousands-of-covid-19-scam-and-malware-sites-are-being-created-on-a-daily-basis/

[2] https://research.nccgroup.com/2020/03/19/threat-actors-exploiting-the-pandemic/

2. GUIDANCE AND ADVICE

This section contains specific advice and guidance to different critical teams and groups within an organization.

2.1. C-suite

2.1.1. Business continuity

F-Secure recommends verifying that relevant business continuity plans (BCP) are suitable for handling the current unusual circumstances. The plans should ensure the following:

- Delegates are in place for roles that are business-critical in case of illness or quarantine that would limit effective work performance.
- Crisis management groups and clear roles for its members for each business-critical area or process.
- One centralized source of COVID-19 related information, which is clearly communicated to all employees in order to mitigate phishing attempts
    - Ideally this would be an internal email address specifically created for this purpose
    - A secondary source would be an intranet page, but without the centralized email address, this could be easily abused by targeted phishing with domain squatting techniques
- Coordinate with the business critical supply chain partners and third parties to ensure that they are still able to provide the required services and that they also have business continuity plans in place and that they are operational despite the Covid-19 impacts in their respective geographical regions[3].

2.1.2. Change fatigue

As more and more users settle in for working from home for the near future, it is important to note that employees getting used to the changes in their ways of working take time. In order to minimize mistakes that could lead to security incidents, it is recommended to let employees adjust to their new ways of working and that leadership are prepared for the employees not to contribute at their normal levels in the beginning.

From a security perspective this is especially important for supporting functions like IT operations and IT security, as they are dealing with an increased number of requests and problems.

[3] See for example https://www.cbsnews.com/news/coronavirus-in-india-possible-tens-of-thousands-more-covid19-cases/ and https://www.mohfw.gov.in/ regarding India. Similar sites are available for other regions.

2.2. IT Operations

2.2.1. Patch management

F-Secure recommends keeping all processes related to security as usual. Most important of all, the normal patch management timelines should be kept and prioritized due to the increased risk of attacks on more exposed and fatigued organizations. This is especially important in the light of recent critical vulnerabilities in products such as Microsoft Windows[4], Citrix[5], firewalls, and VPN concentrators[6].

Patches that should be applied as usual include operating systems (both client and server), critical software as well as security products like AVs, IDS/IPS and EDR software.

2.2.2. Increased event monitoring

Beyond monitoring the usual events on the endpoints and servers, additional checks should be implemented which relate to software used for remote work, such as VPNs and virtual desktops.

In light of recent, critical Citrix vulnerabilities – beyond keeping them up to date – the following indicators of compromise (IOCs) should be monitored, for example using the tool provided by Citrix below.

CVE-2019-19781 (NetScaler ADC): https://github.com/citrix/ioc-scanner-CVE-2019-19781

Additionally, it is recommended for blue teams to pay extra attention to either free or commercial threat intelligence streams and reports to ensure timely changes to the monitoring infrastructure.

2.2.3. Backup incident response suppliers

As even more travel restrictions by countries across the globe are introduced, incident response can become a significant challenge. For a successful incident investigation project, evidence acquisition may have to be performed manually and on-location. This is to ensure that best practices are followed related to chain of custody and that no important evidence is lost.

In order to do so, F-Secure recommends contacting external incident response teams to be on stand-by in all countries/cities where the organization has a presence. This could be done even if there are internal and local capabilities, in case they are incapacitated.

2.2.4. Increased egress filtering

In order to relieve the load on VPNs and to mitigate the chances of a successful command and control (C2) channel for malware to be established, F-Secure recommends using strict egress filtering with deep packet inspection on the VPN concentrators and other network perimeter devices. With this in place certain bandwidth-heavy online services can also be blocked, such as streaming and gaming services. It is also recommended to only allow communication on known and approved ports, such as HTTPS (with the traffic inspected – dependent upon local privacy laws).

[4] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200005
[5] https://support.citrix.com/article/CTX267027
[6] https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

2.2.5. Accommodating a remote workforce

Managed personal devices

F-Secure recommends encouraging employees to use company managed hardware to perform their work from their homes. When this is not possible due to the limited supply of mobile hardware, like laptops; it is recommended for employees to install Mobile Device Management solutions (if available) on their personal devices that will be used for work purposes. As an example, instead of accessing e-mail from untrusted personal laptops, it is recommended to use tablets or phones with an MDM policy installed that was approved by IT security in the organization.

It is important to note however, that the productivity of employees might experience a dip if forced to use phones and tablets for emails.

Additionally, if a pre-existing MDM solution and configuration does not exist, it is ill-advised to rush a project in order to onboard one in a short timeframe. In this case, either personal devices should be used in their current state with increased monitoring capabilities on the affected internal resources, or a limited capacity should be accepted by the business.

Supply chain

To support the now largely remote work force, organizations are looking to purchase or lease more mobile equipment, such as laptops. However, due to the increased demand, some suppliers are running out of stock, forcing some companies to rely on unapproved vendors. F-Secure advises against using such non-approved partners as they are likely to introduce non-standard equipment into the infrastructure, which will have an impact on security. The reason for this is that different manufacturers provide different hardware, firmware and software functionalities in their laptops, which change the attack surface and risk register of an established IT organization. For example, unapproved devices could introduce vulnerable vendor firmware and software[7][8].

VPN

When VPN is used as the main channel for remote employees to connect to the corporate network, it is crucial that these VPNs are used in full tunnel mode. This is to ensure that proper ingress and egress filtering can be applied by the organisation, as all traffic will be funnelled toward the VPN concentrators, as opposed to split-tunnel mode, where only certain traffic will go through the VPN tunnel.

Additionally, full tunnel mode also decreases to risk of information leakage and successful command and control (C2) channels used by malware (when proper egress filtering with HTTPS deep packet inspection is also applied).

2.2.6. Communication

A reliable online communication platform is vital for a remote workforce. In case the organization does not have a single unified communications channel, employees will face unnecessary challenges in case of an incident. In normal working conditions, employees ensure fast and accurate communication by meeting in

[7] https://newsroom.intel.com/news/important-security-information-intel-manageability-firmware/
[8] https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00354.html

person, which is not possible when they are working remotely. This is especially important in case of an increase in phishing campaigns.

F-Secure recommend the following:

- One main online communication channel that is communicated to the employees in order to avoid information to be lost in a remote working environment.
- Failover communication channels in case the main channels experience degraded service due to the heavy load.
- For broadcast messages and important company-wide information email should be used.
    - Dedicated email addresses should be set up for important information, such as HR messages, crisis management team communications and similar, and this email address needs to be communicated to lower the likelihood of a successful phishing campaigns.

2.3. Employees working from home

Various resources can be found online with generic advice and tips for employees[9] switching to working from home. This section is meant to provide more detailed advice to the organization to better support their employees working from home.

2.3.1. Social media platforms

Employees working from home might be tempted to use open social media platforms (Facebook, Twitter, etc.) for work. This is especially true in case the work networks are congested, and the internal instant messaging solutions are unreliable for the increased number of meetings.

It is recommended to take extra care not to share work information on social media, even in ephemeral channels, such as video meetings and similar. To facilitate this, F-Secure recommends employees not to use any social media accounts on work devices and to take extra care where documents and other files are shared.

2.3.2. Home networks

Home networks, in the vast majority of cases, are built using consumer equipment, which are less likely to have the same security maturity or configurability as corporate network equipment. Additionally, it is usually rare that network segmentation is configured on home networks. This means that in case public and unpatched vulnerabilities are exploited by generic malware or targeted attacks, corporate equipment is also at risk.

In order to mitigate the risk posed by insecure home networks, F-Secure recommends the following:

- Require remote workers to use hardened company computers with always-on, full tunnel VPNs.
- In case there are not enough laptops for all employees, personal devices may be used with a properly configured MDM policy.
- Multi Factor Authentication (MFA) should be enabled on all accounts and resources that support it.
- Security software that perform device health checks on private computers used for work purposes should be evaluated and implemented if possible.
    - An example would be: https://duo.com/docs/device-health

2.3.3. Personal devices

Just like in the corporate infrastructure, ensuring that employees keep their personal devices up-to-date they use to access work resources with the relevant security patches is crucial. The best way to achieve this is with MDM policies.

Alternatively, security health checks[10] performed regularly on personal devices can decrease the likelihood of compromise.

[9] https://blog.f-secure.com/cyber-security-for-working-from-home/
[10] For iOS: https://iverify.trailofbits.com/

Lastly, as malware persistence can be a significant challenge on some operating systems and device platforms, reminding employees to perform daily power cycles on all their devices can further decrease the chances of a security incident to escalate.

2.3.4. Security awareness

F-Secure recommends to notify/remind employees about the risks described in this document in order to improve their security awareness in these rapidly changing work environments.

If there are internal or external resources used as training for security awareness, F-Secure suggests to require employees to do them again as they are transitioning into a remote work environment.