CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

CERT-EU Security Guidance 20-001

Cyber Security Guidance to Survive the COVID-19 Crisis

CERT-EU Team

ver. **1.2**
24-03-2020

Contents

1 Introduction

In the context of the coronavirus outbreak, CERT-EU is taking the necessary measures to assess the cyber aspects of this occurrence.

Our various teams have established a plan to address any potential threats that may affect the cyber security and the interests of the European Union Institutions, Bodies and Agencies (EU-I). The purpose of this document is to highlight the various elements of the plan and provide a series of recommendations. We hope that they would be useful to our CSIRT peers and partners to better defend their respective constituencies and help them deal with the cyber aspects of the COVID-19 crisis.

Important: Please note that, in CERT-EU's case, the primary responsibility for maintaining cybersecurity lies with each individual EU-I. Our role consists of supporting our constituents to the best of our abilities and within the confines of our mandate.

2 How to Manage the Crisis

Best practices on preparation for a crisis management strategy demand well-balanced decisions that take into account three pillars:

1. Available resources (human resources, time and money)
2. Exposure to risks
3. Potential Impacts of those risks

The following practical steps should help you deal with the crisis:

1. **Establish Communications**
   a) Establish clear internal communication channels between the infrastructure, the security team and management and monitor them on a regular basis. Define secure backup channels for communication if current IT systems used for this purpose are unavailable.
   b) Be aware of the communication means that you can use to reach your national or governmental CSIRT.
   c) Ensure that you have access to all available communication means with your national or governmental CSIRT in order to reduce response times and improve efficiency.
2. **Identify Relevant Stakeholders**
   a) Within your organisation.
   b) Within your respective business sector(s).
   c) Engage your national or governmental CSIRT in your crisis response plan as soon as possible.
3. **Incident Response Process**
   a) Establish an internal incident response process including procedures, key members of staff and tools that would enable this process.
   b) Be aware of any potential cascading effects of a cyber security breach due to ad hoc measures such as VPN access.
   c) Be familiar with the incident reporting mechanisms to your national or governmental CSIRT, as detailed below.

3 The Cyber Threat Landscape

Overall, The Cyber Threat Landscape as relating to the coronavirus appears to be revolving around the following subjects. CERT-EU intends to continue its close monitoring and reporting on the evolving threat landscape, at the very least with a weekly **COVID-19 Cyber Bulletin** as well as additional reporting as required. The bulletin is shared with our constituents and a number of trusted groups such as the CSIRTs Network.

3.1 Phishing Emails

COVID-19 themed phishing emails abound and use subjects such as:

- Disease center alerts
- Information on the spread of the coronavirus
- Expert protection advice
- Analyses on impacts to economic sectors or to other areas
- Offers to invest in *cures*, vaccines, wonder medicine and other protection products
- *Interesting* facts/videos about the disease
- Strong statements on the *origin* of the virus, pointing to the human responsibility of certain countries
- Misleading stories on the number of victims, how a government is handling the situation, etc., aiming to spread fear and discontent

Beyond the actual spurious content of the phishing emails, these also present the risk of delivering malware, including ransomware, either from attachments or by following download links, as well as deceiving users into supplying personal, banking or professional credentials.

3.2 Spreading Disinformation

Several disinformation campaigns for political purposes, and conducted via legitimate platforms (hijacked or controlled by non-EU media) or fake accounts have been spotted.

The aim of disinformation campaigns so far has been either to "worsen the impact of the coronavirus, generate panic and sow distrust" or to generate alternative narratives concerning the origin of the virus (e.g. engineered by Western countries).

3.3 Malicious Applications

Several malicious applications on computer systems or mobile devices have been observed. There are cases of applications that offer to provide useful coronavirus-related information (e.g. track the virus outbreak, track symptoms) that in reality have malicious intent.

3.4 Possible Intrusion and Information Exfiltration Attempts

Beware of possible intrusion and information exfiltration attempts. In CERT-EU's case, EU-I directly involved in the crisis response might be particularly targeted by such attempts.

The motive behind these attempts may be to collect information on the extent and management of the pandemic or of gaining access to scientific knowledge valuable to third countries for developing their own expertise or for possible commercial use. Intrusion attempts may simply

have as an objective to disrupt the organisation's operation(s) and impede coronavirus mitigation efforts. The latter case may involve less sophisticated efforts such as destructive malware (wipers) and ransomware.

3.5 Other Threats

Additional items, still relevant in the current situation, are:

- Threats against VPNs, video conferencing systems and messaging apps. CERT-EU is monitoring these threats for its constituency and reporting as required.
- Proliferation of the usage of alternative tools by end users (any kind of collaborative platform, conferencing, chatting, etc.) that involves a threat in terms of losing the confidentiality of sensitive information. Constituents can deploy technical solutions (e.g.enforce encryption in wikis in Microsoft Teams) and make users aware of these risks.

4 Improving Monitoring and Detection

4.1 Virtual Private Networks (VPNs)

As a lot of organisations use VPNs for teleworking, malicious cyber actors focus on identifying and targeting their vulnerabilities. If your VPN solution does not use Multi-Factor Authentication (MFA), you may seek assistance, if applicable, from your national or governmental CSIRT to assess which additional measures are feasible.

Teleworking can also raise problems in terms of **capacity** on your VPN infrastructure. If you need to deploy new infrastructure, please respect the security processes and procedures in order not to compromise the security of the existing one. You are strongly advised to monitor newly discovered vulnerabilities in VPN products in a timely manner so you can patch or mitigate them.

If applicable, your national or governmental CSIRT can also help you collect the necessary logs from VPN servers to enhance the existing monitoring and detection capabilities.

4.2 Cloud Systems

If you use cloud services then it is best practice that **privileged accounts** shall be accessed only with MFA. If MFA is not possible, then you should consider at least conditional access. If applicable, your national or governmental CSIRT may be able to help you collect logs from O365 and Azure Management plane to enhance the existing monitoring and detection capabilities.

4.3 Endpoints

The risk of compromising Windows endpoints is significantly higher when teleworking staff use laptops under a Split VPN setup that allows a mobile user to access dissimilar security domains like the internet and your organisation's network at the same time. To reinforce the security of your endpoints, ensure that the built-in Windows firewall or a similar solution is activated. The procedure for updating endpoints while being remote from the main corporate infrastructure for a long time must be reviewed, taking into consideration the implications

of the available bandwidth and mitigating the risks associated with limited patching (to save bandwidth) or configuring endpoints to get their patches directly from software vendors (as their update infrastructures could be compromised).

If possible, endpoint logging must be activated and/or reinforced. If applicable, your national or governmental CSIRT may help you collect the relevant endpoint logs to enhance the existing monitoring and detection capabilities.

4.4 Email Systems

Web access to email systems (e.g. Outlook Web Access) should be closely monitored, especially if MFA is not in place. If applicable, your national or governmental CSIRT may help you collect and analyse email logs.

4.5 Web Applications

If it is absolutely necessary to expose more web applications to the Internet to cope with business needs during the crisis, please consider the following key points:

1. If possible, enable MFA. Otherwise monitor access logs more closely.
2. Ensure that software components are up to date, and access to the administration pages is restricted and HTTPS is enforced.

Proactive and periodic monitoring of internet-facing assets should be reinforced and extended. Shadow IT is of particular concern as business owners and users, as they adjust to their new teleworking conditions and the pressure of getting their job done, might use non-corporate solutions or applications, unbeknownst to their IT and security teams.

If you have not done a recent security assessment for any newly exposed web application, you should determine whether a quick security scan for critical vulnerabilities is feasible under the current conditions and seek, if applicable, the advice of your national or governmental CSIRT.

5 Reporting Incidents

If applicable, incidents should be reported to your national or governmental CSIRT using the proper reporting channels and procedures.

COVID-19 Incidents

In CERT-EU's case, EU-I are instructed to report incidents by email. If the incident is linked to COVID-19, they are asked to mention it in the subject of their email and it will be assigned priority status.

For example, EU-I are asked to provide CERT-EU with at least the following information in case of an emergency:

1. Contact details and organisational information – name of person, organisation name and address, email address, telephone number.
2. Short summary of the incident/emergency/crisis, type of event.
3. Source of the event/incident (e.g. the system produced an alert, etc.).
4. Affected system(s) (e.g. network asset, etc.).

5. Estimated impact (e.g. loss of communications, etc.).
6. Additional information such as:
    a) Details of the observations that led to the discovery of the incident - scanning results (if any); an extract from the log showing the problem, etc.
    b) In case there is a need to forward any suspicious emails to CERT-EU, all email headers, body and any attachments should be included.

6 User Awareness

Cybercriminals are skilled at exploiting people when they are at their most vulnerable and COVID-19 is a dramatic event. We highly recommend that you send an awareness message to end users to follow the simple steps that go a long way towards protecting themselves while teleworking:

- Be vigilant about attempts of **social engineering** (including phishings, fake IT Helpdesk calls, fake mobile applications, etc.). If in doubt, call the sender and trust your instincts. **Do not hesitate to exchange with people on the phone** to check if the requests are legitimate. Many malicious actors are trying to leverage the situation to commit frauds and extortions.
- **Enable automatic updating** on your devices so they are always running the latest version of the operating system and anti-malware.
- Refrain from **unnecessarily burdening your professional network** (e.g. cameras can be switched off during videoconferences). If you experience **slowness on the network**, have you thought about checking whether your roommates are not using all the bandwidth at home? Streaming, online gaming or downloading can surcharge your home network and can lead to disconnections during your professional interactions. If this is not the case, contact your IT support to find a solution.
- When teleworking, you might **receive calls from people pretending to be calling from *Microsoft* or *the helpdesk*** proposing to help out with apparent issues with your PC. In case of doubt when called, you should hang up and call the number of your helpdesk to check with them.
- **Do not upload work-related information and crisis procedures to social networks or platforms that have not been validated by your IT staff.**
- **Stay calm** if you cannot connect to the network of your organisation. Do some tasks you can manage offline and try to connect later. Do not revert to other, less secure solutions for your professional exchanges.
- **Use encrypted drives**, where available, to store and exchange sensitive non-classified documents.
- **Talk to your children** about cyber safety. Listen to their online experiences and explain to them the importance of staying safe in the digital world as well offline.

7 Lessons Learned

- Share the lessons you learned while coping with the ongoing crisis with your peers and your national or governmental CSIRT. In CERT-EU's case, EU-I can use a dedicated chat platform for timely help or advice. **We are stronger together**.
- After the crisis, take time to **review all the procedures, processes and controls** that were (mis)used or ignored.

- Identify all those that were missing, update all infrastructure documentation accordingly and **apply those** that had been bypassed during the crisis.

8 Additional Resources

- SANS Security Awareness Deployment Guide – Securely Working at Home, SANS Institute.
- Zero Trust Architecture, NIST Special Publication 800-207, 2nd Draft.
- CORONAVIRUS / COVID-19 : Appel au renforcement des mesures de vigilance cybersécurité, Cybermalveillance.gouv.fr. French only.
- COVID-19 and the shift to remote work, ESET.
- TR-59 - Remote Work - In times of a crisis, CIRCL.
- Public Awareness and Prevention Guides, EUROPOL.
- Top Tips for Cybersecurity when Working Remotely, ENISA.
- Recomendaciones de seguridad para situaciones de teletrabajo y refuerzo en vigilancia, CCN-CERT. Spanish only.