SWITCH security report on the latest IT security and privacy trends

March/April 2020

I. The coronavirus has company – a pandemic of computer viruses

The coronavirus pandemic has given Switzerland an unprecedented boost in terms of digitalisation and remote working/computing. Never before have so many Swiss residents worked from home at once. This measure – one that's intended to stop or at least slow the spread of the actual microscopic virus that attacks people and their immune systems – is helping to spread virtual viruses that infect networks, servers, computers, tablets and smartphones.

There are six main reasons behind this development.

1) Many companies and their employees were caught unawares by the Swiss government's request that staff work from home where possible, often with little time to prepare. Many were simply not ready to suddenly start working from home using digital tools, and cybersecurity was rarely their uppermost concern.

2) There are now numerous business devices connected – either wirelessly or by cable – to private networks, under security standards that don't measure up to those implemented by many companies.

3) The security processes that employees go to such effort to learn (no inserting third-party USB sticks, no downloading software that's not been checked and approved by the IT admin, etc.) were soon forgotten like yesterday's news.

4) Decentralisation of devices increases the number of networks involved and exponentially expands the number of targets for cybercriminals.

5) All of a sudden, employees working from home are receiving enquiries, invitations to attend online meetings and requests to send or receive data either from the company they work for or – and this is where things get really risky – from addresses claiming to be from that company. Often, people are unable to distinguish between real and fake.

6) At home, it's far easier to give into the temptation to download private data onto company devices.

Of course, cybercriminals can't pass up an opportunity that suits their purposes so well. On the first day of the lockdown alone, Switzerland's Reporting and Analysis Centre for Information Assurance (MELANI) reported that scammer extortion emails were doing the rounds. A week later, MELANI lamented that the coronavirus was being used as a pretext for an unprecedented number of scams, fakery and phishing attempts. And Emotet, Trickbot and Ryuk – three immensely dangerous pieces of ransomware – are still lurking in the shadows, waiting to paralyse entire networks and blackmail companies and organisations to their breaking point and beyond. We warned about these issues in the SWITCH 6/2019 security report, and among their recent victims is the renowned window manufacturer Swisswindows AG, which is filing for insolvency in Switzerland due to a Ryuk attack.

So the topic of 'cybersecurity when working from home' mustn't be swept under the carpet. Quite the contrary, in fact: awareness is more important than ever. That's why MELANI published an awareness appeal on 24 March 2020 aimed at all those working from home. On 2 April 2020, it published guidelines for end users. As always, you can consult good sources like ibarry.ch and Europol's recommendations for securely working from home. Please refer to the links and the next article.

Read more:

https://www.melani.admin.ch/melani/en/home.html
https://www.heise.de/newsticker/meldung/Abzocke-im-Onlinehandel-Muehsamer-Kampf-gegen-Corona-Geschaefte-4694227.html
https://www.bleepingcomputer.com/news/security/trickbot-emotet-malware-use-coronavirus-news-to-evade-detection/
https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH-Security-Report-2019-06.pdf
https://www.inside-it.ch/de/post/ein-cyber-angriff-hat-uns-in-arge-bedraengnis-gebracht-20200228
https://dataloft.ch/security/schweizer-fensterfirma-swisswindows-ag-geht-nach-ransomware-angriff-pleite
https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/fernzugriff.html
https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/fernzugriff-enduser.html
https://ibarry.ch/en/
https://ibarry.ch/wp-content/uploads/2020/03/safe-at-home_final-1.pdf

II. The ten most important rules for working securely from home

What can companies and their employees do to make teleworking from home as secure as possible? The security checklist on iBarry.ch offers lots of important, basic and useful tips (iBarry is the ‘St Bernard’ that provides protection against the dangers of the internet on behalf of the Swiss Internet Security Alliance, of which SWITCH is also a member; see link below). The SANS Institute has also compiled a guide on working securely from home. Both of these resources are available at the links below. We’ve summarised the most important tips here to give our readers a quick overview:

1) Use your company’s VPN channel for all business activities.

2) Separate your work and your private life as much as possible. Of course ideally you’ll have a designated room or a separate work space and your own device for working (desktop computer, laptop, tablet or smartphone).

3) Protect business devices and documents from unauthorised access – even from your housemates, children or partners, depending on the security level.

4) Remain vigilant when it comes to third-party emails, prompts to make changes to your devices or software, or invitations to load additional programs.

5) Treat supposed ‘coronavirus specials’ with suspicion – these are frequently being used to phish data or infect devices with malware too.

6) Secure your computer or device with a strong password.

7) Use external storage devices to back up your data (hard drives, USB sticks, etc.) and encrypt them as well.

8) Encrypt all sensitive data on clients.

9) Protect all business devices from misuse with strong authentication – e.g. two-factor authentication using both your device and an SMS code sent to your mobile phone.

10) Observe the security rules that apply in your company, even when you’re at home.

Read more:

https://ibarry.ch/en/digital-security/
https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit
https://security-awareness.sans.org/sites/default/files/2020-03/01-SSA-Coronavirus-WorkingFromHome-DeploymentGuide_English%20UK_0.pdf
https://www.sans.org/sites/default/files/2020-03/03-SSA-Coronavirus%20-WorkingFromHome-CheatSheet_English%20UK.pdf

III. Online meetings – how secure are Cisco Webex and Zoom?

Online meeting software is in greater demand than ever before. But many experts are also pointing out that two of the most popular applications have privacy and/or security issues – in their free or low-budget versions, at least.

Take Cisco’s online meeting service Webex, for instance. It reserves the right to collect and store data, as well as to share it with third parties. From the Cisco Webex Meetings privacy data sheet: ‘We may share Registration Information, Host Information, and/or Usage Information with service providers, contractors or other third parties to assist in providing and improving the service.’

Several vulnerabilities have been discovered in Webex too. Attackers may even manage to use both the Webex Network Recording Player and the Cisco Webex player to access and remotely control devices to a greater or lesser extent to execute whatever code they like on the target user’s system.

Another very popular meeting service is even more enthusiastic when it comes to collecting data: Zoom. The list of data that Zoom collects according to its own privacy policy covers several screen pages (see the link below). What’s more, Zoom has already fallen victim to a major hack. And, if all that weren’t enough, dataloft.ch reports that investigative journalists from ‘The Intercept’ are claiming that Zoom’s statement that meetings are end-to-end encrypted is based on Zoom’s own definition of end-to-end encryption, which does not admit hackers but theoretically allows the provider to access unencrypted video and audio data from meetings.

And indeed, analysing Zoom in more detail reveals a few privacy issues, as well as bugs that pose certain security risks on both Windows and Mac OS. On the other hand, since

Zoom is perfectly suitable for large online meetings and lectures, many people still don't want to do without the web-based service, or cannot. And actually, you don't need to do without it – as long as you observe the following seven security instructions:

1) Prior to using cloud services, develop or update a usage concept that outlines topics such as data protection, data classification, what data may not be processed/stored in the cloud under any circumstances, etc.
2) Make sure you always have the latest version of Zoom.
3) Don't announce Zoom meetings publicly (on Twitter, LinkedIn, etc.).
4) Generate random Zoom meeting IDs.
5) Protect your meetings with a password.
6) Manage attendance at your meetings; start with your microphone muted and video stopped. Set up a waiting room for the participants then let them into the meeting one by one. Click on the 'Lock Meeting' button when all the participants are in the meeting. Then restart the camera and unmute the microphone before beginning the meeting.
7) Never use Facebook or Google login credentials; instead, assign dedicated username/password combinations for logging in.

Read more:

https://www.linkedin.com/pulse/using-google-meet-zoom-webex-other-video-conferencing-jeffrey-carr/?published=t
https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-cisco-webex-network-recording-player-and-cisco-webex-player-could-allow-for-arbitrary-code-execution_2020-032
https://zoom.us/privacy
https://dataloft.ch/security/end-to-end-verschluesselung-von-zoom-unter-beschuss

IV. For real? Ransomware gangs develop a 'code of honour' in the coronavirus pandemic

We'll refrain from commenting on the following piece of news, but believe it's worth mentioning all the same; our esteemed readers can make up their own minds. According to a report on bleepingcomputer.com, the cybercriminal organisations CLOP Ransomware, DoppelPaymer Ransomware, Maze Ransomware, Nefilim Ransomware and Netwalker Ransomware have agreed to suspend attacks on hospitals, medical facilities and other health organisations during the Covid-19 pandemic. And they stressed to the site, almost in unison, that they'd never deliberately attack hospitals anyway. But anyone hoping that the coronavirus is making cybercriminals go soft is in for a disappointment. When asked what would happen to those hospitals whose data had been 'accidentally' encrypted, a representative of Netwalker Ransomware once again revealed the ugly face of cybercrime: 'If someone is encrypted, then he must pay for the decryption.' Say no more!

Read more:

https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

This SWITCH security report was written by Dieter Brecheis and Michael Fuchs.

The SWITCH security report discusses current topics in the field of cybersecurity. It is aimed at all interested internet users, and seeks to make them aware of current threats. Despite careful review, SWITCH accepts no liability for accuracy.