:: Positive Technologies

Work from home: digital distancing to keep your network safe

positive-tech.com

As COVID-19 continues its spread around the world, and society becomes more locked down, many companies are asking their employees to work from home to reduce the risk of coronavirus spreading among employees and the wider population. But we cannot forget about the increased risks of digital infection for businesses—cyber attackers now have more points of entry into local networks than before.

IT and security teams will have their hands full trying to ensure operational continuity and block unauthorized access to company systems. To help them, we have compiled some recommendations to keep in mind when moving their company to telework, plus a checklist to make sure they have all of their security bases covered.

Securing workstations

The first step is to determine whether employees will be working on a company laptop, a company desktop brought in from the office, or by remotely connecting from a personal device (aka BYOD or "bring your own device"). Different security measures are appropriate for each of these situations.

The safest option is to have employees work on a company laptop. This allows the company to make sure in advance that the laptop meets all the requirements for remote workstation security (for example, installing corporate antivirus protection and other necessary software, plus enabling two-factor authentication, full-disk encryption, event logging, and automatic updates). However, when employees use their own devices, companies will have a difficult time enforcing these measures and almost certainly cannot verify compliance further down the road. An attacker could, for example, place malware on the employee's personal device or steal their credentials in a phishing attack.

At a minimum, personal devices should have antivirus protection and the latest updates for their operating system and all software. If this is not possible, the employee should be blocked from connecting to the corporate network from that device—and should ideally be provided a company laptop.

Securing the network perimeter

One of the more secure options for remote access is to use a virtual private network (VPN). Not all VPNs are created equal, so we recommend safer options such as L2TP with IPSec. Another popular option is to connect via Remote Desktop Protocol (RDP).

Whichever one you choose, it's worth also using a special gateway for remote access. For RDP connections, this is called a Remote Desktop Gateway (RDG). For VPNs, this is called a VPN Gateway. We recommend against allowing direct connections to a corporate workstation.

Remote access is particularly dangerous for business-critical networks and systems: telecom management networks (OSS/BSS, MANO), process networks at factories and utility companies, ATM processing and card processing networks at banks, accounting servers, and sensitive filing systems, to name a few.

These networks, which are usually isolated from the Internet and even from the main corporate network, have strict access controls. But when working from home, administrators are tempted to make life easier for themselves by setting up a special connection to manage and configure things remotely.

As a result, businesses should keep a close eye on administrator compliance with security rules. Constant monitoring of the network perimeter, and especially the key segments of it, is a sensible move. They should also scrutinise the use of remote administration software, such as RAdmin and TeamViewer, to see if it is being used for malicious purposes (this can be determined by artifacts in network traffic).

Since contractors cannot make on-site visits due to COVID-19, companies may have to provide special remote access to external companies and integrators. Needless to say, this can create a lot of risk. It is essential to monitor any such connections closely: attacks via trusted connections are one of the most common ways of hacking the networks of major companies.

Segmenting networks

VPNs can be tricky, however. What usually happens is that the VPN is forwarded to a particular segment on the local network; the availability of the other network segments is not guaranteed. So IT departments may be up against the clock to re-configure equipment and tailor VPN access to the precise needs of each user. Rushed for time, they may simply open up access to a subnet not just for individual employees, but for all VPN users. This is bad for security, increasing both the potential reach of external attacks (whenever they breach the local network) and insider attacks. IT teams should preemptively make a plan of action for maintaining network segmentation and allocating sufficient VPN pools.

Securing accounts

Security assessment statistics shows that at least 75 percent of companies use dictionary passwords for their external services (such as websites, portals, databases, and teleconferencing). The danger gets even worse when these weak passwords are used for remote connections to the local network. All an attacker needs to start attacking internal resources directly is to brute-force a weak password.

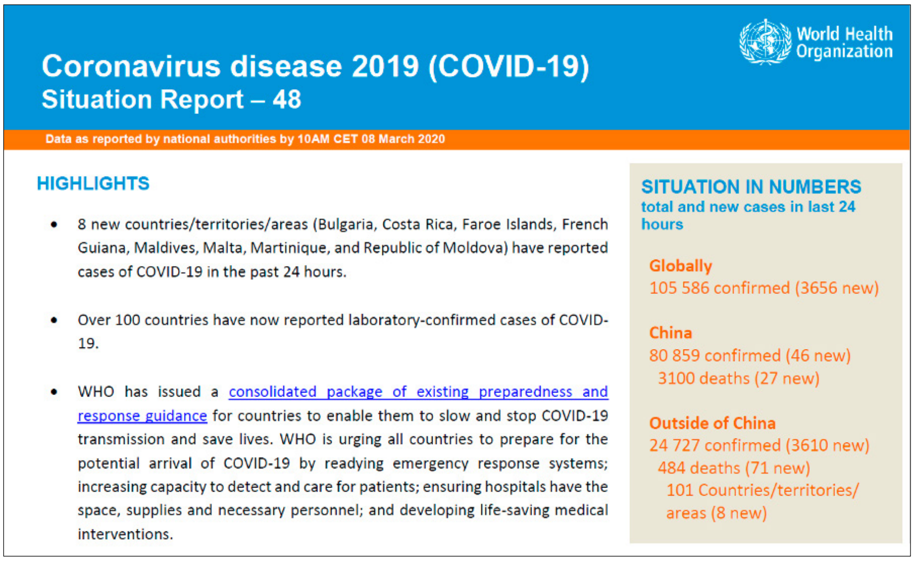
This makes it critical to reinforce password policies when employees work from home. Make sure that passwords are even longer and more complex than usual. For remote work, we recommend passwords at least 12 characters long for non-privileged accounts and at least 15 characters long for administrators. Passwords should contain both upper and lower-case letters, special characters, and numbers. Forbid easy-to-guess passwords.

Before this crisis began, many employees were not given remote access due to the sensitivity of their work. But newly office-free accountants, engineers, technicians, and corporate executives often have little idea of how to stay safe and avoid falling victim online. One predictable consequence is a sharp rise in the number of accounts with easy-to-guess passwords on the network perimeter. IT departments can preempt this by requiring longer passwords. Here is one way to check the complexity of passwords: export password hashes from the domain controller (in ntds.dit) and run this file through password cracking dictionaries.

As another line of defense, consider using two-factor authentication with hardware tokens. This helps even when weak passwords get compromised.

Making common sense common

Already, criminals are taking advantage of the pandemic in phishing emails, fake sites, and booby-trapped mobile apps. Professional APT groups (such as SongXY, Gamaredon, and Higaisa) quickly caught wind of the telework shift and started attacking employees' personal email accounts. One phishing email by unknown perpetrators was even sent to our company in an attempt to steal credentials.



Coronavirus disease 2019 (COVID-19)
Situation Report – 48

World Health Organization

Data as reported by national authorities by 10AM CET 08 March 2020

HIGHLIGHTS

- 8 new countries/territories/areas (Bulgaria, Costa Rica, Faroe Islands, French Guiana, Maldives, Malta, Martinique, and Republic of Moldova) have reported cases of COVID-19 in the past 24 hours.
- Over 100 countries have now reported laboratory-confirmed cases of COVID-19.
- WHO has issued a consolidated package of existing preparedness and response guidance for countries to enable them to slow and stop COVID-19 transmission and save lives. WHO is urging all countries to prepare for the potential arrival of COVID-19 by readying emergency response systems; increasing capacity to detect and care for patients; ensuring hospitals have the space, supplies and necessary personnel; and developing life-saving medical interventions.

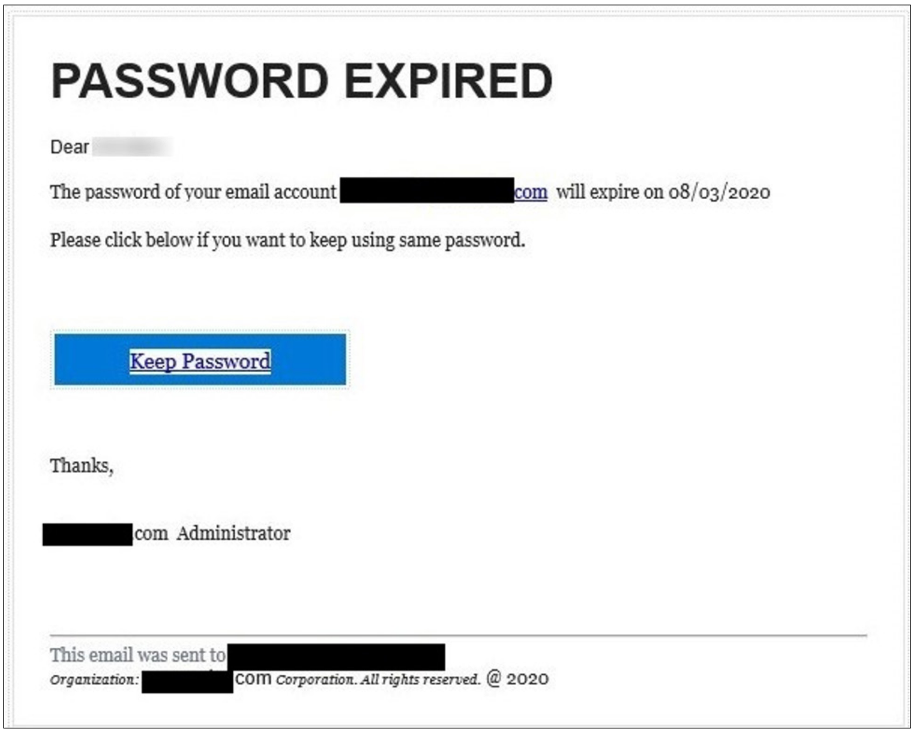
SITUATION IN NUMBERS
total and new cases in last 24 hours

Globally
105 586 confirmed (3656 new)

China
80 859 confirmed (46 new)
3100 deaths (27 new)

Outside of China
24 727 confirmed (3610 new)
484 deaths (71 new)
101 Countries/territories/ areas (8 new)

Figure 1. Phishing page by the Higaisa APT group



PASSWORD EXPIRED

Dear [redacted]

The password of your email account [redacted]com will expire on 08/03/2020

Please click below if you want to keep using same password.

Thanks,

[redacted]com Administrator

This email was sent to [redacted]
Organization: [redacted] com Corporation. All rights reserved. @ 2020

Figure 2. Phishing attempt against Positive Technologies employees

Employees must be vigilant and aware of the threats, as they distinguish phishing messages from legitimate ones. Doing so requires holding conversations, providing well-designed training materials that are not overwhelming, and giving tips related to information security and social engineering. It is also worthwhile to perform dynamic scanning of all incoming email attachments inside a sandbox.

Work-from-home security checklist

To make sure you haven't forgotten any of the big factors during this massive work-from-home transition, here is a brief checklist. Compare to see if your company's security is where it needs to be.

	What to do	Why to do it
1.	Verify and strengthen password policy	An attacker could penetrate the company's local network by brute-forcing an employee's account
2.	Minimize access rights to internal resources (allow only what employees actually need)	An insider or external attacker could steal sensitive information by penetrating the local network from an employee's home computer

	What to do	Why to do it
3.	Secure employee devices used to connect to the corporate network. Scan email attachments in a sandbox. Train employees on security and help them avoid becoming a victim of a phishing attack.	An employee's device could be infected with malware. This device could spread the malware to the local network.
4.	Monitor the network perimeter non-stop	An external attacker could penetrate the local network if insecure remote access interfaces or services are on the network perimeter
5.	For remote connections, use gateways instead of a specific workstation	Employee workstations could be compromised in a targeted attack on network interfaces that are open to remote connections
6.	Log security events on workstations and servers on the local network, employees' remote devices, and protection systems. Retain copies of network traffic. Monitor security events on key systems. Perform automated deep analysis of network traffic.	Improper employee actions and attacks on corporate resources cannot be monitored. Incident reaction and investigation could be delayed.
7.	Have a security operations center (SOC) or special staff on call to monitor protection 24 hours a day	Response to any detected security incidents could be delayed. Cyberattacks cannot be stopped in time.
8.	Maintain segmentation of internal networks. Strictly control access to key segments and systems.	Key business systems could be compromised by an external or internal attacker
9.	Maintain extra capacity for handling the loads caused by employees working remotely	Business processes could be disrupted if employees cannot connect to internal corporate resources
10.	Have the IT department available with 24-hour technical support to keep infrastructure functioning	Business processes could be intentionally disrupted by denial of service or account lockouts. Business processes could be unintentionally brought down by overwhelming employee network demand.

What to expect

COVID-19 is at the center of the media's attention. Attackers will inevitably twist it to their advantage through phishing lures to employees' corporate and personal email addresses, as well as their social media pages. Working from home means weaker digital security and better odds for attackers. We expect a sharp rise in attacks on the network perimeter of companies and remote workstations of employees.

In many countries, organisations where working from home had never been an option (such as government agencies and research laboratories) are suddenly at high risk. The rushed nature of this change will inevitably cause mistakes by administrators and an increase in insecure systems. Employees with poor security awareness who previously had worked only in an office could unwittingly be of great use to attackers - the insider threat is increasing as well. Attackers are eager to pounce on these weaknesses. The consequences for companies could be catastrophic. If your company is not yet ready for remote work, we urge not acting in haste: build a process that is comprehensive and well thought-out, in a way that accounts for the full spectrum of security threats.

Double monitoring efforts of network activity of employees and all remote connections, monitoring of security events on key business systems, and monitoring of the network perimeter and employee workstations—these are all key components of a plan for reducing the risk of a network breach by an external attacker. Equally critical is the willingness of employees to step up and combat the constant threat of phishing.