ISSN 2738-7097 https://doi.org/10.11610/cybsec03

British Embassy Sofia

Cybersecurity Newsletters

IICT Institute of Information and Communication Technologies

UK-BG Partnership in Cyber Security for SME and Organizations

Newsletter November 2020 Number 3

Aims and Scope

Contents:

The current online newsletter is focused on the topic challenges related to the protection of employees' home networks and how smart devices changing the threat pattern associated with data sharing. Due the COVID-19 crisis, many security and IT teams have to support and protect employees who must work remotely.

The practical recommendations from security experts toward the mitigating risks to enterprise security from home networks and smart-home devices are presented. Eight practical recommendations for remote workers' protection are given from the security experts. In this respect, a strong policy for all home employees should involve the usage of an antivirus tool on the machines that access the organization's resources. Consideration should be given to implementing alternative cloud-based workstation monitoring tools. An overview of supported console tools and required licenses to access non-domain computers should be done. A quick decision is to set up tools such as Splashtop SOS or LogmeinRescue to allow IT support team to remotely access employees' home machines to assist in setting up remote access.

In the current issue the **CounterCraft** company that is a pioneering provider of cyber deception and counterintelligence products to detect targeted attacks is presented. CounterCraft's solution deploys deception-based campaigns and offers deep monitoring and complex response actions. The Cyber Deception Platform is used by government's law enforcement agencies.

Some useful information about the problems of secure remote work is given by providing free e-books and free cybersecurity toolkits that will help to protect and manage remote workers. Remote workforce security tips and best practices from 8 security pros can be found too. Finally, some additional news and security tips about remote working at home is given. A list of links to Bulgarian, UK and international cyber-related institutions are also presented.

Issue Editors: **Prof. Daniela Borissova, DSc**
Zornitsa Dimitrova, PhD Student

Issue Focus: Challenges Related to the Protection of Employees' Home Networks and How Smart Devices are Changing the Threat Pattern Associated with Data Sharing

Prof. Daniela Borissova,
CIO at IICT, Issue Editor

Zornitsa Dimitrova
PhD at IICT, Issue Editor

Remote work is not a new challenge. Many companies were already embracing remote work to give employees a better balance between work and life, along this contributes to reduce the carbon footprint and drive corporate efficiencies. Due to the Covid-19 pandemic situation worldwide, remote work has become a necessity for modern organizations looking to create business continuity plans. This is related to many IT challenges in today's reality of remote workers.

From an IT perspective, there are a lot of unknowns involved with managing remote work:

- Home Wi-Fi networks and routers are more easily compromised than the enterprise-grade equipment in offices, which increases the risk of exposure and inadvertent leaking of corporate and customer data.
- More and more data are stored in the cloud and this essential element should be properly secured using suitable strategies.
- Corporate VPNs are rarely robust enough to respond to the growth in remote access to the network. This can affect performance, which further complicates data protection.
- The Emails exchanges will increase, due to the absence of in-person communications, and also contributes to increases the likelihood that email will contain sensitive information along with potential personal data.
- The widespread use of tools for videoconferencing remotely will lead to a drain on bandwidth in many regions, so people will rely on email communications during peak hours.

From the comfort of their home office, employees may fail to take precautions such as using only corporate email. Instead, they might send work files over their personal email to get work done faster – a practice that puts corporate information at risk.

The VPN should be used for applications with remote access. VPNs provide a flexible connection to a variety of services (web pages, email, a SQL server, etc.) and can protect your traffic. Keep in mind that not all VPNs are worth the money; it’s a good idea to evaluate your must-haves before you choose a VPN technology. Keep in mind that VPN services provided for privacy purposes only protect the data to and from the VPN provider, not to the destination so are not suitable for protecting remote access. For some use cases, it is possible also to be set up the encrypted remote connections into a remote desktop or other individual server. Many of these types of connections (RDP, HTTPS, SSH) include encryption as part of their service direction and do not require an additional VPN or other encryption service to secure the data-in-transit.

Everyone needs a remote work security policy. Organizations should develop a remote work security policy to refresh and inform employees of what’s expected of them when working remotely. For example, it is good practice to provide access to corporate resources only to those employees who use business email accounts and to block all others. The same applies to the use of video conferencing systems in organizing seminars, lectures, tests, and more. The applicability of this rule has been proven in the

practice of the conducted lectures and tests during the latest 2 semesters at the University of Library and Information Technologies. Unfortunately, some organizations with an insufficient level of competence allow the use of personal e-mail addresses for business correspondence. The users working from home need to be aware of the home network risks and should be trained by the organizations on how to mitigate them. In this regard, during the conference **DIGILIENCE'2020** on the 1st of October, a round table was conducted with a focus on the role and responsibilities of the CIO. Along with CIO responsibilities the needed attention was given also to the role of CISO, where the main contributions are to ensure information and data security. In addition to the important role of CIO and CISO, a CIO/CDO online training course is planned on18 of January 2021. The lecturer will be Prof. Siraj Shaikh – Professor of Systems Security at the Institute of Future Transport and Cities (IFTC) at Coventry University (UK).

Eight Practical Recommendations for Remote Workers Protection

8 Key Security Considerations for Protecting Remote Workers
(from: **csoonline.com**)

Many employees at businesses worldwide have been forced to work from home because of COVID-19 related social distancing mandates. This trend heightens the need for organizations to pay more attention to the security of home networks and of the smart-home products and other devices connected to them, analysts say. Home routers, printers, security systems, DVRs, gaming consoles and other smart devices can significantly change the threat model for the corporate network.

Many security and IT teams suddenly have to support and protect employees who must work remotely due to the COVID-19 crisis. Here are some areas that should be covered:

1. Determine what endpoint protection you will require for home users. While you may have consoles and the ability to manage all the workstations at your physical office, you do not have the same level of control for home computers. Windows Defender included in Windows 10 is a more than acceptable antivirus tool for a remote machine. Any remote worker that has a Macintosh should not be exempt from using endpoint protection software. One in ten Mac users have been attacked by the **Shlayer Trojan**.

2. Review what software remote employees need. For Office 365 subscribers, **some** of the licenses allow you to install the Office suite on up to five PCs or Macs, five tablets and five smartphones. Those with Volume licenses can allow **Office for home use** purchases for your employees. You may need to review your options and licensing alternatives based on what platform and version of Office you are currently licensed for.

3. Ensure remote access does not introduce more risk. You may have to suddenly set up and license remote access servers, Windows 10 virtual desktops or other remote technologies. Don't introduce more risk in terms of licensing and security risks based on the decisions you make. For remote access that includes remote access services, remember that ransomware attackers look and scan for **open RDP servers,** targeting anything responding on port 3389. Don't move RDP to another port as TSgrinder scans for an RDP response on any port.

4. Implement two-factor authentication (2FA). When adding more remote access solutions, consider adding **2FA** to remote access solutions. You can easily add 2FA solutions such as DUO.com to existing on-premises remote access solutions. DUO.com can add 2FA to

RDGateway and Remote Web Access solutions. While your organization may need to move quickly to allow your staff to work remotely, you can still ensure that only those admins and users are allowed in and not any attackers as well.

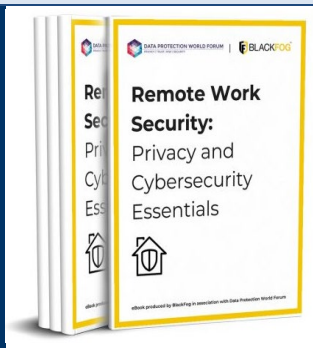
5. Use a virtual private network (VPN). Recently there have been several **high-profile vulnerabilities** in VPN software. Often on client workstations that have not been updated in years, an older version of VPN software has been left behind. Ensure that your VPN solutions are up to date both on the server or firewall that is providing the VPN solutions, or on the desktops of the remote user.

6. Assess the impact to firewalls, conditional access policies and other logging. Your organization might have a security information and event management (**SIEM**) logging solution that looks at traffic coming from local desktops and laptops to server resources. If your entire workforce traffic suddenly comes in from various IP addresses, your logging platform data will no longer be "normal".

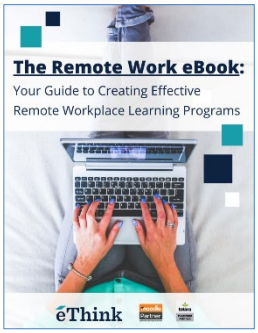
7. Educate employees on COVID-19 scams. The National Cyber Awareness system warned of **COVID-19 scams** that are circulating. Urge your users to not click on unsolicited emails and to use only official websites. Ensure that the firm has a central online bulletin board that they go to for official communication and notification, especially if anyone in your organization becomes infected.

8. Update acceptable use policies for employees. Finally, ensure your acceptable computer use policies cover employees' home computer assets. If this wording is not already there, you'll need to quickly get up to speed in allowing employee's personal assets to be used for remote access. You'll need to work with the organization's attorneys and tax advisors to see if the use of personal computers and personal phones of the employees mandate a need for reimbursement for use.

Useful e-books & Tools for Secure Remote Work



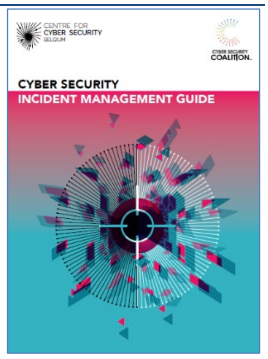
eBook: Remote Work Security – Privacy and Cybersecurity Essentials



The Remote Work eBook: Your Guide to Creating Effective Remote Workplace Learning Programs

Remote Working Successfully – EBook. Implement and Perfect your Remote Working Setup

CYBER SECURITY INCIDENT MANAGEMENT GUIDE



Managing Remote Workers: Free Toolkit.

The following free cyber security toolkits will help to protect and manage remote workers:

- Free tools for: Employees and Contractors Working Remotely
- Free tools for: IT Professionals Accessing Privileged Accounts Remotely
- Free tools for: IT Professionals to Secure Remote Workstations

Remote Workforce Security Tips & Best Practices – 18 security pros share their top tips and best practices for securing a remote workforce.

Some News and Security Tips about Home Working

Remote Workplace Infrastructure is Identified as One of Global Top Ten Technology Risks for 2021

The annual ISACA/Protiviti Global Survey of IT Leaders and Professionals identifies the top ten technological risks and challenges for organizations in 2021. The ninth place is for Remote Workplace Infrastructure. The organization lacks sufficient tools, technologies and resources to enable and support a remote workforce for an extended period with necessary levels of control. **ISACA and Protiviti risk survey report ...**

SASE could bolster security for remote workers

The coronavirus pandemic has accelerated some companies' plans to adopt secure access service edge (SASE). Gartner coined the term SASE, pronounced "sassy" to describe a technology category that converges network and security services, including SD-WAN, secure web gateway (SWG), cloud access security broker (CASB), DNS protection, and cloud-based firewall. For new SASE customers, the biggest delay is typically on the hardware side. Employees may need new SASE edge devices to handle networking and security in employee homes. But there are also ways to deploy SASE without any new hardware. CloudCheckr, software company that makes cloud management tools, uses Zscaler's SASE platform to connect its employees to the cloud services they need to do their jobs, including AWS infrastructure, in a secure way.

NetworkWorld/Gartner report ...

The Cybersecurity Pandora's Box. How Remote Working Poses Security Risks for Organizations

The transition to remote work amid COVID-19 opened a cybersecurity Pandora's box with security and compliance gaps surfacing, paving the way for potential data breaches. For example, the SailPoint study shows that 1 in 3 US employees (33%) use their own personal devices for remote work This was a significant difference when compared to EMEA and ANZ, where half of the employees reported remote work was conducted via employer-supplied technology. Over half of EMEA and ANZ respondents (51%) experienced a phishing attack since the pandemic began.

SailPoint report ...

Online Security Tips for Working from Home during Covid-19 Pandemic

Once upon a time, working from home was a luxury. Now, it's become a necessity for employees. Here are the top ten things you should be aware of to ensure you and your staff are sticking to a sensible work from home security policy: 1) Invest in comprehensive antivirus software; 2) Keep family members away from work devices; 3) Invest in a sliding webcam cover; 4) Make sure your company VPN is as strong as can be; 5) Use a centralized storage solution; 6) Secure your home wireless network; 7) Be aware of videoconferencing security risks; 8) Make sure your passwords are strong and secure; 9) Maximize security around online banking; 10) Pay attention to email security.

Kaspersky report ...

Cyber Institutions & Initiatives in UK & Bulgaria

CounterCraft

CounterCraft is a pioneering provider of cyber deception and counterintelligence products to detect targeted attacks.

Advanced adversaries and targeted attacks threaten large organisations on a daily basis. CounterCraft provides a distributed Deception Platform that creates automated digital breadcrumbs to bait adversaries into thinking they are penetrating companies' networks. This innovative cybersecurity approach allows CounterCraft to get information on attackers' and objectives while misdirecting them.

Counterintelligence campaigns are time-consuming to design and complex to deploy and maintain. Monitoring them can be an arduous, if not impossible task. It is difficult to evaluate the success of a campaign and deliver useful intelligence as an output.

CounterCraft's solution deploys deception-based campaigns and offers deep monitoring and complex response actions. The Cyber Deception Platform is currently used by governments, law enforcement agencies, and Fortune 500 companies – proving craft and expertise in IT security. It runs automated counterintelligence to discover targeted attacks with a real-time active response and zero false positives.

Links to Cyber Related Institutions

Links to Bulgarian, UK & International bodies

- ENISA – European Union Agency for Cybersecurity
- ISACA international professional association focused on IT governance
- ECSO coordinate the development of the European Cybersecurity Ecosystem
- Cybercrime.bg
- CounterCraft
- ESI CEE

Feedback

For questions & recommendations

E-mail: acerta@bas.bg

Editorial Board

Academic CERT association under an agreement signed from a group of academic bodies (IICT, DI, ESI as a first step) to strengthen cooperation in cyber-security related research

The publication of the newsletter is supported by the British Embassy in Sofia.

The opinions in the newsletter reflect the authors' point of view.

British Embassy Sofia

IICT Institute of Information and Communication Technologies

Bulgarian Defense Institute

ESI European Software Institute Center Eastern Europe

СЪЮЗ ЗА СТОПАНСКА ИНИЦИАТИВА
UNION FOR PRIVATE ECONOMIC ENTERPRISE

DIGILIENCE Conference Series https://digilience.org