Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
Sophisticated adversaries such as Avivore are extremely resourceful and will tailor the techniques used to the victim environment. This means that they will rarely use all the capabilities within their arsenal in a single intrusion, nor will they limit themselves to only previously observed techniques.

The future of Avivore

Avivore remains active and the sectors it has targeted remain a high priority for critical networks. However, the current climate created by the arrival of Covid-19 may have had some impact on the level of activity – not least because supply chains are not as active. But it is likely that Avivore and other groups employing similar techniques are turning their attention to other high-priority sectors and regions.

The particular TTPs used by Avivore, along with a growing understanding of its victims’ environments, make it highly likely that it would be able to remain under the radar and retain access to other connected victims, potentially in other sectors, without detection.

Aside from leveraging certain custom capabilities, Avivore’s approach, which is heavily based on ‘living off the land’ and abuse of legitimate/native functionality, is becoming widely used, and therefore it is becoming increasingly difficult to be certain who exactly is conducting intrusions – Avivore or other actors. Attribution has always been a challenge for the cyber security industry and it’s not getting any easier.

About the author

Oliver Fay is a principal consultant in the Response & Advisory team at Context Information Security (www.contextis.com) and leads the company’s Technical Threat Intelligence Services. He manages the delivery of complex analysis and threat intelligence projects and is a CREST Certified Threat Intelligence Manager.

References

1. ‘Context Identifies new AVIVORE threat group’. Context Information Security, 3 Oct 2019. Accessed Jul 2020. www.contextis.com/en/news/context-identifies-new-avivore-threat-group.
2. Mitre ATT&CK, home page. Accessed Jul 2020. https://attack.mitre.org/.

GDPR in the new remote-working normal

Marc Lueck, Zscaler

Since May 2018, the General Data Protection Regulation (GDPR) has required any organisation doing business with European citizens to make significant changes to its data processes. Over the two years since it came into law, it has ushered in a new level of data hygiene to enterprises.

This was not a painless process, however. Organisations globally went through the often costly exercise of ensuring they had an overview of personal information, as well as implementing tools to be able to process and store that data in a secure manner.

When the GDPR came into force, many organisations quickly deployed best-of-breed security tools to keep their data secure. At that time, the focus was predominantly limited to office boundaries. Now, with current social distancing guidelines forcing huge swathes of the workforce to work remotely, and potentially shifting business focus away from the office environment in the future, organisations are having to revisit their initial efforts and ensure that compliance with GDPR can still be achieved in this new normal. What follows are guidelines as to how organisations can ensure this.

Impact assessments

Businesses that already had processes and policies in place for remote working are in the enviable position of merely having to ensure that those policies and rules are in use by their staff working from home. However, those organisations which have only had an onsite workforce or offered limited flexible working will need to identify if en masse working from home impacts or changes risk levels. This will require opening up their records of processing activities and each of their data protection impact assessments (DPIA).

A DPIA is a process to identify data protection and privacy risk and address them accordingly. Under GDPR, where processing operations present specific risks to individuals’ privacy rights due to their nature, scope or purpose, controllers carry out an assessment of the impact of the proposed processing operations on the protection of personal data.

It’s key to note that a DPIA is an ongoing process, and as any project develops or a new situation arises, new risks might be identified. Means to avoid those risks must also be found. When an organisation is making significant changes to an existing system or process – as might be the case with remote working – it’s necessary to revisit the DPIAs and
check whether the new situation and processes are already covered or not.

“Thanks to technology, employees can stay productive while out of the office. However, it needs to be ensured that the private work environment keeps any accessed and processed data as secure as in a corporate office”

As the aim of a DPIA is to identify and analyse how data privacy might be affected by differing actions or activities when working from home, companies are responsible for ensuring that the appropriate controls are in place when personal information is accessed or processed from a home environment, and that the information is handled no differently than it was from the office.

Data privacy in remote working

What complicates matters for businesses with the current situation is the sheer scale of the issue. Over the past few months it has become clear that, thanks to technology, employees can stay productive while out of the office. However, it needs to be ensured that the private work environment also keeps any accessed and processed data as secure as in a corporate office. With the global Covid-19 situation forcing all members of a household to stay at home wherever possible, each individual environment has to be evaluated.

Questions that a business may not have considered suddenly become of the utmost importance. What does the workplace look like when working from home? Is there a physical office available, or a cupboard or closet that can be locked in order to guarantee privacy of data and devices? Are there children in the household, and if so, is the device or devices the employee uses for work used for other purposes? It’s all too tempting to allow the family to use a work laptop, or to use it for casual private browsing. Conversely, security risks can also be introduced in the opposite way – if private devices that might not be equipped with security tools are used for work purposes.

Organisations are therefore having to revisit their security posture to provide a safe remote-working experience that prevents data breaches. Not only should they address vulnerabilities to their own networks and the physical storage of data, they will have to face the fact that remote workers will inevitably have to move data between the corporate network, the cloud and the personal laptop. To protect personal data in transit from one location to another, GDPR suggests encryption to protect privacy and security and prevent leakage.

Five-step plan

Not all of an organisation’s employees will be accessing sensitive personal information while they are working from home. The changes needed are more granular and, first and foremost, an organisation has to figure out which employees are dealing with sensitive information.

Step 1: Reopen your DPIA. The first step for an organisation is figuring out where you need to apply this remote-working policy. That means a DPIA has to be reopened to understand the impact of the new environment of remote working. During this process the organisation can gain insight into which employees access sensitive personal information while working from home, and subsequently create various risk categories for the remote workforce.

Step 2: Ascertaining the physical requirements of the home office. Based on the impact of the DPIA mentioned above, new controls may need to be applied specifically for that identified category of employees dealing with sensitive information while working remotely. Organisations have to figure out what the home office has to look like for the different categories of remote workers.

When looking at the physical security of a remote workplace, organisations have to take different measures into account based on the risk categorisation. That might start with having a separate room at home that can be locked at the lighter end of the scale, and range up to video surveillance for the highest security category.

Step 3: IT security for the home office. The biggest challenge in a remote office scenario is arguably maintaining visibility into the data traffic and devices so as to prevent threats. Both data controllers and data processors have to implement appropriate technical and organisational measures to ensure the same level of security in the home office environment as in the corporate office, and which is also appropriate to the risk categorisation level.

At a minimum, remote employees will require secure access to the resources they need in the corporate datacentre or the cloud. Additionally, data governance has to be applied to make sure that the data stays where it is supposed to stay and is not copied locally.

Step 4: User awareness of remote working policy. All of these steps until now will be for nothing if organisations don’t ensure that their remote employees are aware and conscious of the business’s acceptable use policies (AUPs). Keeping data privacy an ongoing cultural element of remote working is key. All those employees dealing with sensitive information must ensure that nobody else in the family deals with the devices that access or process any of this data. Consistent reminders of this fact may seem like nagging, but without this awareness the whole system falls apart.

Step 5: Training employees. Last but not least, the pandemic situation calls for an urgent rethinking of general security training. In the past few months we’ve seen bad actors attempting to capitalise on these times of uncertainty and fear to spread new malware campaigns and take advantage of the remote working situation. Organisations should switch up their security training as well. Open and frequent communication with
Facing ransomware: an approach with private cloud and sentinel software

Holzen A Martinez-Garcia, TecNM/Technological Higher Institute Progreso

Data and information are assets that carry a high value for organisations – and cyber criminals know this. They try to take advantage of this fact and have adopted various hacking techniques. One of the most current and dangerous is the infection of devices with cryptographic ransomware. Currently there are many approaches to countering this threat focused on the detection and mitigation of risks, but only a few of them consider an imminent infection and take proactive data recovery techniques.

Ransomware is a type of malware that uses encryption algorithms and techniques to hijack a virtual computer asset, such as data or operating system functionalities. The modus operandi of this type of malicious software consists of encrypting files on the disk or blocking access to the system completely or partially until the user pays the creator of the malware, usually with a digital currency such as Bitcoin. According to Bhardwal et al, ransomware is a digital extortion that: infects a computer system; attacks from a variety of vectors; and can be implemented via browser exploits, the downloading and installation of freeware applications, through email attachments and ads that offer cash and other incentives to invite potential victims to fall for the deception.¹

The uncertain new normal

This all may seem like a lot of work – and it is. But organisations can take some comfort that these efforts to revisit GDPR compliance are worth the effort. As and when we gradually emerge from the global pandemic, working from anywhere is predicted to become a core part of the new normal, and the processes laid down today will remain relevant for years to come.

Even if the majority of the workforce does indeed choose to return to the office, an organisation can be confident that it’s prepared, should any similar event happen in future, and that it can offer more-flexible working practices should its employees demand it.

About the author

Marc Lueck is CISO EMEA at Zscaler (www.zscaler.com). He is a senior security practitioner with over 20 years’ experience across multiple industry sectors, from financial services to publishing, specialising in enterprise security management, threat intelligence, compliance and security architecture.

How the proposal works

This work presents an approach based on a generic network architecture that consists of an adaptable private cloud that contains a Linux-based storage server with open-source sync file software included. This stores real-time versioned copies of the files synchronised with the endpoint devices. The client layer also contains installed sync and share software, and sentinel software – specifically designed software that emerged as a product of this research. Figure 1 describes the proposal graphically.

The sentinel software works like a monitor of the folders on the client device previously configured by the user. The language used for coding was C# .NET and its main function is to block the monitored folders when there is suspicion of an imminent file infection.

¹Social engineering techniques can be varied, with a lot of crossover between methods and their use.