CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

No 10 / May 2021

Recent Cyber Events:

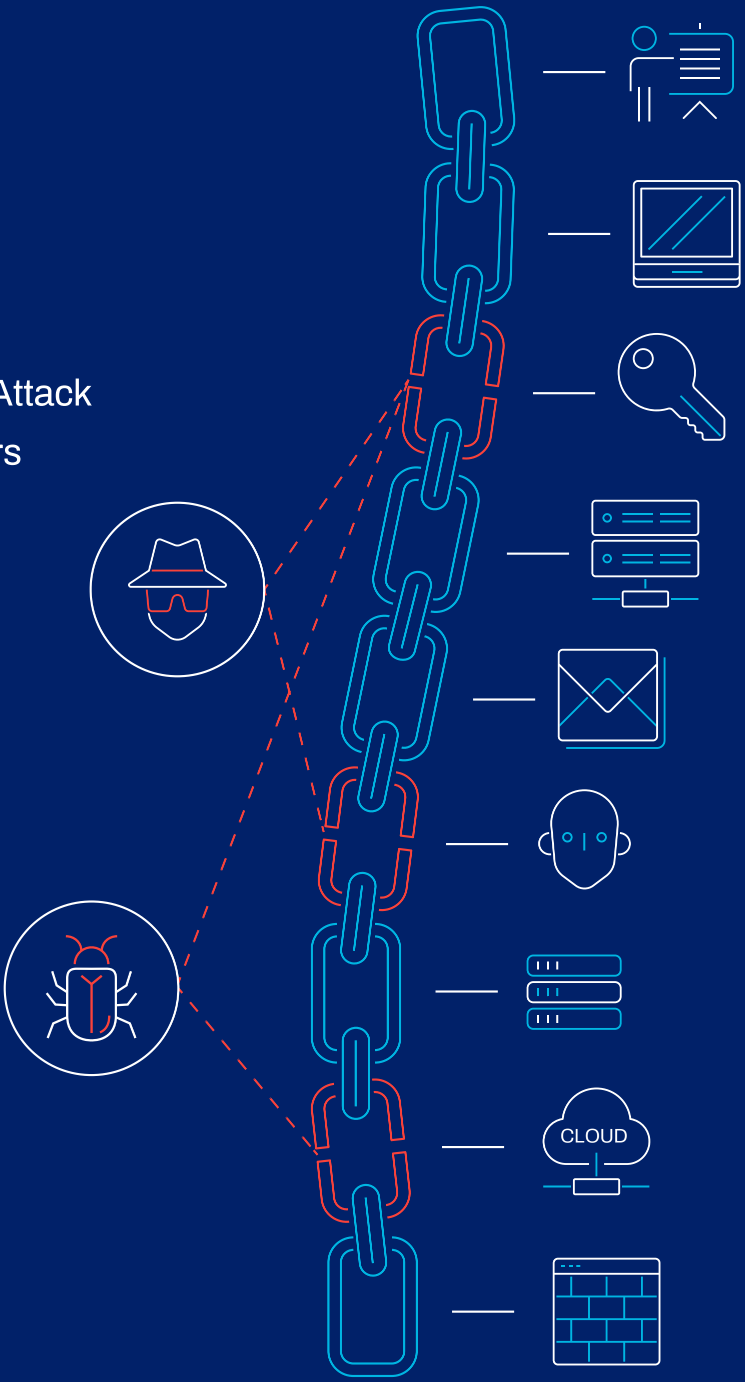
Considerations for Military and National Security Decision Makers

The Software Supply Chain:

→ The SolarWinds Supply Chain Attack

→ Did Leaked Code Help Attackers Breach Exchange?

→ Supply Chain Vulnerabilities and Open-Source Software



Other topics in this issue:

→ Responding to the SolarWinds Attack

→ Leaked Facebook Data May Be Used for Phishing

→ China-India Relations and Cyber Events

→ Remote Working Increasing Cyber Risk

→ Cyber Exercises for the Strategic Level

Published by CCDCOE

ABOUT THIS PAPER

This recurring report is the collaborative view of NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) researchers highlighting the potential effects of current events and developments in cyberspace on armed forces, national security and critical infrastructure, based on publicly available information. It does not set out to be exhaustive. While the authors have made every effort to describe events from a perspective relevant to NATO and partner nations, there may be national and regional differences which this paper does not address.

The authors of this paper are independent researchers at the NATO CCDCOE; they do not represent NATO, nor does this paper reflect NATO's position. The aim of the paper is not to replace information about vulnerabilities and incidents provided by CSIRTs and providers of CIS products and services.

Lessons identified from the SolarWinds supply chain attack

'You can't trust code that you did not totally create yourself. […] No amount of source-level verification or scrutiny will protect you from using untrusted code.' (Ken Thompson)

Much has been written about the SolarWinds incident, which has been characterised as a supply chain attack. This supply chain attack targeted the process by which a trusted organisation updates software for their clients. The effect of an attack on a single organisation can be multiplied by the number of clients the organisation serves. SolarWinds was likely picked as the vehicle to distribute the backdoor because of who their customers were.

In Recent Cyber Events No 8, we explored some of the problems raised by this incident and some of the considerations regarding recovering from a major breach like this. What is clear is that the security measures taken by SolarWinds were not sufficient to prevent or detect the attack. To manipulate the update packages, and to avoid detection, the attackers used some sophisticated techniques.

Understanding how the supply chain may be compromised is important for organisations procuring or maintaining software so that they can assess the security measures taken across the supply chain. It is also of interest to anyone developing or customising software in-house.

The attackers chose to target a specific stage in the building of update packages, which may have helped to keep it undetected for so long. Perhaps the most obvious way to manipulate software is to alter the source code. [1] This can be done either by an insider or by hacking into the development network of the software company. The source code, with the malicious modifications, is then compiled by the developers into machine code and combined with other parts when building the package to be distributed to the customers. The source code is, however, often read by many people in the development team so any major changes such as including a complex piece of malware runs a high risk of being detected.

The attacker could also target the finished update package just before distribution, replacing it with one that has the malware included. This has the advantage of usually being on an internet-connected download site that may be easier to compromise than a developer's network. There is, however, a significant risk of being detected here as well. The integrity of the distributed packages may be checked by validating digital signatures or by comparing the packages to the master on the internal development network.

According to research by CrowdStrike, the SolarWinds hackers took a different path. They installed malware onto the servers at SolarWinds where the update packages are built from the source code. Whenever this malware detected a specific source code file being compiled, it would insert the backdoor code. This way the malware was never present in the source code and the developers believed that the package included only authorised code.

The tactic is reminiscent of the techniques used by Stuxnet, where malicious code for the industrial controllers was inserted in a similar way. This highlights the need for the protection of the complete development environment and distribution infrastructure. If the integrity of the software used to build software cannot be guaranteed, we cannot ensure the integrity of the software built using it. This is not a new realisation; it was pointed out very clearly by Ken Thompson as long ago as 1984.

[1] Source code is the human readable computer code written by programmers in programming languages like Java. It has to be translated, compiled, into code that the computer can execute.

This is, of course, not the only point in the software supply chain that may be attacked. Any intermediary handling the software package, such as a reseller or systems integrator or even your own IT department, may be targeted and checks need to be performed to ensure the integrity of the software through the entire chain.

There is also the possibility of attacks even earlier in the chain. Most software packages include software libraries that are sourced from other suppliers. In many cases, these are open-source libraries, but they can also be licensed by commercial developers. In either case, they may be compromised in ways such that every piece of software they are included in will contain malicious functionality.

Finally, there is also the question of end users. If end users are not prevented from installing software by technical security measures, they may be tricked into installing software if the attacker can make them believe that it is a legitimate software update. One example is a recently reported attempt to trick Android phone users to install malware masquerading as a system update.

Since complete trust in software will be impossible to achieve in most cases, a defence-in-depth strategy must be employed. The outer defences will be the vetting and auditing of suppliers, making sure that they are trustworthy and that they apply reasonable security measures in safeguarding their development environment. The next is the measures taken to ensure the integrity of the software when delivered and its protection until it is installed.[2] The keep of the fortress is the mindset of not trusting something just because it is on your network and its battlements the measures taken to mitigate the threat from malicious software running in your environment.[3] Even with those defences in place, breaches through the supply chain may happen. Building resilience so that operations can be sustained even with parts of the IT infrastructure affected by malicious activity should always complement the pure cybersecurity measures.

Did leaked code help attackers breach Exchange servers?

It has been difficult to miss the reports of extensive attacks leveraging a recently discovered vulnerability in Microsoft Exchange. Virtually every organisation running their own Exchange server was vulnerable and thousands of servers were attacked, most notably by the group dubbed Hafnium.

That an exploitable vulnerability is present in a complex piece of software like Exchange is not surprising. When it is discovered by malicious actors and exploited before it can be patched, the consequences can be devastating. Luckily, mature and responsible software suppliers have processes to manage vulnerabilities as soon as they are discovered and reported, whether by in-house researchers, by other cybersecurity experts or by users.

The process usually includes verifying the vulnerability, assessing its potential impact, locating its cause and developing and releasing a software update or patch fixing the issue or releasing advice to users on how to mitigate it by other means. As part of the process, information about the vulnerability may be shared with partners such as cybersecurity companies or CSIRTs before a patch is available.

Did something go wrong in this process when Microsoft researched the Exchange vulnerability? Some reports suggest that proof-of-concept code may have leaked and that it may have assisted threat actors in developing their attacks. This could explain why so many hacker groups seem to have been able to exploit the vulnerability so quickly. If so, the very process designed to mitigate the risks from the vulnerability may instead have aggravated the problem until the patch was released and for those users that did not promptly apply the patch.

According to the Wall Street Journal, Microsoft has found no indication of leaks from inside the company but did shared information, including proof-of-concept code, with partners in its Microsoft Active Protections Program (MAPP). Proof-of-concept code is developed to better understand and demonstrate how the vulnerability can be exploited, but in the wrong hands, it can also be adapted to exploit the vulnerability.

Interestingly, one of the Russian companies recently sanctioned in the wake of the SolarWinds attack was reportedly a Microsoft security partner. It was sanctioned for providing support to the Russian Intelligence Services' cyber programme. Microsoft has said it will comply with the sanctions and the company will be removed from the list of companies' receiving early access to vulnerability information from Microsoft.

So, while there is undoubtedly value in involving many parties in the remediation process, gathering the information needed to address the problem and giving key players time to prepare must be done with utmost care. What organisations can be trusted with the information? At what point in time during the process is it safe to release sensitive information?

There is a lucrative black market for vulnerabilities and exploit code, so there is a financial incentive for untrustworthy players in the chain to leak information. There may also be actors that, voluntarily or involuntarily, act on behalf of a state with a different view on information security and responsible behaviour in cyberspace.

[2] This should include, but not be limited to, the use of digital signatures to verify integrity.

[3] These practices are often referred to as the Zero-Trust Model.

The typical software supply chain attack is about injecting malicious code in the supply chain to leverage when attacking users of the software. The problem, in this case, was not the protection of the integrity of the software update, but it may have been a failure in protecting the confidentiality of the information used when developing the update.

These types of attacks show the attack surfaces of the software supply chain and how attackers can spread attacks widely by applying the right leverage at the right place in the chain. However, it is also entirely possible to execute targeted attacks through the software supply chain. Questions about the extent to which individuals in the chain can be trusted should also be asked by military decision-makers. In the case of Exchange, the sphere of influence may be relatively small, but almost all systems are dependent on software which may be vulnerable to software supply chain attacks.

The US Cybersecurity & Infrastructure Security Agency (CISA) offers publicly accessible remediation steps for the Microsoft Exchange vulnerability and explains the consequences and approach and provides resources for leaders and IT staff.

On vulnerabilities in the software supply chain and open-source software

The French Information Systems Security Agency (ANSSI) released a report that gives details about an intrusion campaign of software by French IT company Centreon. According to ANSSI, the campaign caused breaches in several French entities from 2017 to 2020 and ANSSI was able to find backdoors on compromised systems. Centreon sent out a press release stating, *inter alia*, that no customers were affected, and that about 15 entities using an unsupported, obsolete open-source version had been. It went on that the incident is not a supply chain type attack and that the company did not distribute malicious code.

While the attack may not have been against Centreon's commercial supply chain, it could still be characterised as a supply chain attack. According to the US Committee on National Security Systems' (CNSS) Glossary, supply chain attacks are defined as:

> **'Attacks that allow the adversary to utilise implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.' (CNSS)**

Whether or not the compromised software was commercial or unsupported open-source, the incident shines a light on a central problem: the use of third-party software and code in products and its side effects. The use of third-party software components may bring particular vulnerabilities with it, meaning that a great degree of trust is placed in the hands of the software author and possibly no transparency is provided. However, outsourcing software production or parts of it, relying on code libraries or using pre-built code is not new and is practised by all kinds of organisations of all sizes. As early as ten years ago, InfoWorld reported that between 30 and 70 per cent of the code in programs comes from third parties. From a security perspective, there are two obvious factors to consider: In the case of using code from a third-party, the degree of trust placed in the other party's code. If software production is outsourced, then the trust level of the external company must be determined as well. While the use of open-source code also brings many advantages, such as full access to the source code and possibility to do security audits on it and having a large community of users being able to spot any malicious injects, there is no immunity to supply chain attacks and because of its popularity, open-source code software can become a target for supply chain attacks itself. According to Naked Security, there was an attempted supply chain attack on the open-source programming language PHP in March in which the source code was modified by imposters. The malicious code would have opened backdoors on servers using PHP Zlib compression, but the changes were noticed and rolled back before the next official release.

The attacks discussed here are the non-physical type of attacks on supply chains, those on the so-called software supply chain. As defined by a report of the Atlantic Council

on software supply chains:

> **'A software supply chain attack occurs when an attacker accesses and modifies software in the complex software development supply chain to compromise a target farther down on the chain by inserting their own malicious code.' (Atlantic Council (2020): Breaking trust: Shades of crisis across an insecure software supply chain)**

An attacker's decision to focus on the software part of the supply chain can be especially apparent when you consider how widely the attack can spread. For example, the attackers on the PHP code could have compromised a vast number of servers in a single attack. Another example that illustrates the scalability of such attacks is the incident involving ASUS software updates in 2019. According to Motherboard, after an attack on the company's servers, the malware was believed to have been loaded onto the devices of hundreds of thousands of customers through an automated software update tool.

Not only is good protection and a solid framework to protect national supply chains from cyberattacks and tampering needed, but so is attention to the software. A strong framework should not only take care of the security of the code but also define the extent to which data may be passed on to third parties, especially for servers in other nations.

The fact that open-source code can be reviewed freely by anyone may be a security advantage, but other things work in the opposite direction such as the difficulty in establishing the exact origin of the code and what development practices were used and perhaps a manufacturer not taking responsibility to fix security issues as they are discovered. These risks need to be evaluated and, if possible, mitigated before a decision to use open-source software in critical applications is taken. The US Department of Defense (DoD), for example, gives a good overview of issues to consider and measures to take regarding the use of open-source code and third-party code.

Responding to the SolarWinds attack

Since the discovery of the SolarWinds supply chain attack, the US and its NATO Allies have been working hard to identify the extent of the compromise and mitigate its effects. Information has been shared extensively between public and private investigating entities and guidance has been made available to the public and kept updated.

Russia's role in the SolarWinds breach was suspected from early on. On 15 April, the UK's GCHQ National Cyber Security Centre (NCSC) confirmed that Russia's Foreign Intelligence Service (SVR) was behind the SolarWinds compromise and a series of other cyber intrusions. In the US, the National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) issued a joint advisory exposing the activities of the SVR, including the SolarWinds compromise, targeting US and allied networks. These incidents are part of a wider pattern of cyber intrusions by the SVR which have previously attempted to gain access to governments across Europe and those of NATO members. On the same day, the US and the UK also formally attributed the attacks to Russia.

The media has been expectant that the US would 'retaliate' over the intrusions. There were reports, citing unnamed US officials, of the US planning 'aggressive' action against Russia and talk of punishing President Putin, although the actions were expected to be combined with economic sanctions. Even President Biden's statements about a 'need to disrupt and deter our adversaries' and 'imposing substantial costs' may be interpreted as indicating some sort of offensive response in cyberspace.

> **'The UK will continue to work with allies to call out Russia's malign behaviour where we see it.' (Foreign Secretary Dominic Raab)**

On 15 April, however, the US and UK response followed more established patterns in responding not only to the SolarWinds attack but to a whole range of harmful activities they attribute to the Russian Intelligence Services.

Calling out malicious behaviour. Both nations took to the established pattern of calling out Russia for its aggressive behaviour in cyberspace and confirmed their commitment to work with international partners to continue to defend against Russia's attempts to destabilise western societies.

Public exposure. The UK government also publicly exposed parts of the Russian Intelligence Service's cyber structures, similar to the Estonian Foreign Intelligence Service's report in 2018.

Economic sanctions. The objective of President Biden's executive order was to impose costs 'in a strategic and economically impactful manner' on Russia for the destabilising international actions.

Diplomatic action. In addition to the sanctions, the US also expelled ten Russian diplomats from Washington DC.

Expressions of solidarity. NATO's North Atlantic Council (NAC) and the EU High Representative both issued statements in solidarity with the US, as did other nations including Canada and Australia.

> **'Now is the time to de-escalate. The way forward is through thoughtful dialogue and diplomatic process.' (President Joe Biden)**

The statement from the NAC makes it clear that NATO is open to dialogue with Russia 'when that is possible' and President Biden voiced similar hopes in an interview. What is also clear from these statements is the ambition to continue to advance responsible state behaviour in cyberspace.

The steps taken by the US point to the public's expectation of cyber retaliation perhaps being misguided. Retaliation is understood as taking action in return against the perpetrators of an attack against you to inflict similar harm on them. Even though action in cyberspace may seem like the most obvious retaliation for a cyberattack, it could just as well be done in another domain.

However, if the US intelligence community had undertaken a cyber response against the Russian government as a covert operation, this information would likely not have been disclosed publicly, and some experts believe that there may have been 'unseen' responses and that more may still come.

Outside of unfriendly but lawful steps such as the imposition of sanctions, both international treaty and customary law are plain that using force or similarly intrusive, potentially damaging measures are only accepted to end ongoing breaches, not as a means of retaliation.[4] With the SolarWinds campaign, which by nature can be considered espionage, the debate is still open whether it constitutes an international wrongful act at all and what the basis of the US response is, something that has been explored in an article on Lawfare. The scope and scale of the compromise, cost of mitigation for the victims and the risks that the breach posed to the global technology supply chain are factors that challenge easy dismissal of the case as 'mere espionage'.

In any case, there are significant risks in taking retaliatory cyber action. It may fail to produce the sought-after damaging effects and may backfire and cause damage to one's own or one's partners' systems or cause indiscriminate collateral damage. With retaliation in cyberspace, there is also the possibility that the exploit could be re-engineered to be used against oneself in the future. The most serious risk, however, may be the risk of escalating the situation rather than deterring future attacks.

Attribution is a prerequisite for countermeasures, but it also has its own significance in terms of calling out perpetrators and signalling the authority of international law. The message will be most powerful when attribution is done by partners and allies together. Imposing costs for malicious actions is also important and has been stressed in the comments of many political leaders. This can be done with means other than cyberattacks and without violating international law. The US and its allies have a history of combining economic sanctions and public exposure of Russia's cyber capabilities and command structures.

Rather than quickly deciding to retaliate by cyber operations, it may be wise to consider overall geopolitical objectives instead of narrow cyber aims, and to attempt to consolidate the simultaneous objectives of deterrence and dialogue when deciding on how to respond to unfriendly state activity in cyberspace.

The US position was one taken between a rock and a hard place: while defending national security and national interests, they acknowledged an aspiration to keep a dialogue open with Russia and avoid further destabilisation in cyberspace.

Leaked Facebook data may be used for phishing campaigns

According to FORTUNE, Facebook suffered a data leak that exposed the data of over 500 million users of the platform. With this, Facebook is in the news again after the Congressional hearings in 2018 concerning Cambridge Analytica where 87 million users' data were accessed and another data exposure of 267 million users in 2019. Business Insider reported that a user posted the data including phone numbers, Facebook ID, names, birthdates and bios, sometimes with email addresses, locations and birthdates, on an online hacker board. A Facebook spokesperson reportedly told the news outlet that the data could have been scraped because of a vulnerability patched in 2019. According to Wired, Facebook has suffered many breaches[5] in the past but it appears that this data is a different set than those from earlier reported leaks. There seem to be some high-profile profiles among the data such as the US Secretary of Transportation, the EU Commissioner for data protection, several US officials and Facebook CEO Mark Zuckerberg himself. An interesting side note is that, according to Business Today, Zuckerberg seems to be using the cross-platform centralised encrypted messaging service, Signal. Facebook's own messaging service WhatsApp was making headlines because of its updated privacy policy, making some users switch to alternatives such as Telegram and Signal.

'A data leak of information on approximately 533 million Facebook users – including profile names, mobile numbers and location data – has prompted talk of regulatory action against the social media platform, but bringing a case under Europe's General Data Protection Regulation (GDPR) may not be successful or possible.' (Computer Weekly)

Computer Weekly reports that Ireland's Data Protection Commission began to investigate but that there is a possibility that no regulatory action is possible since the scraping appears to precede GDPR.

With the vast amount of leaked data, it would not be surprising if there will be a rise in phishing attempts on victims of the leak. The leaked data now available to hostile actors gives much room for elaborate social engineering attacks combining the information and possibly posing as trusted individuals or institutions proving credibility through scraped data. Phone numbers associated with email addresses can prove particularly useful to hostile actors since they can trick victims into providing reset and confirmation codes. The heightened amount of data available to misuse means that the need for vigilance is heightened as well. If armed forces or defence members have registered with either official email addresses or business phones, targeted and tailored attacks may be possible. To confirm if the leak might affect individuals and in turn their affiliated organisation, the data itself can be consulted. Alternatively, 'have I been pwned' offers a searchable database for leaks in general including the functionality to search by phone number and Mozilla offers

[4] See The Charter of the United Nations (Art. 2(4) and 51) and Articles on the Responsibility of States for Internationally Wrongful Acts (ASR) (ASR is widely considered to be customary law).

[5] See also MySpace, Yahoo!, VK.com or LinkedIn for further information on data leaks and scraping.

a similar service called Monitor. Both have been updated with data from the Facebook leak.

To protect armed forces personnel, decision-makers may want to consider policies and guidelines concerning personnel representation on social media. Decisions should be made based on the effect that a leak would have, exposing military or defence personnel. Does your organisation generally allow members to indicate their professional role or post pictures and information related to defence activities such as profile pictures in uniform or to use organisational email addresses and business phone numbers? Is there a possibility that malicious actors could use this information to demoralise, for example, deployed personnel or their families? A strong regulatory and policy framework balancing free speech and other rights with security is needed to protect personnel and defence organisations online. Information provided online should not be considered private or deletable as such leaks show.

More information about risks concerning the data industry can be found in the NATO StratCom COE Data Brokers and Security - Risks and vulnerabilities related to commercially available data report including a comprehensive risk taxonomy. Taking things further, NATO StratCom COE also released a report named Camouflage for the Digital Domain - A force protection framework for armed forces addressing digital risks and threats in cyberspace as well as issues of mobile phones during exercises and malicious use of digital information.

China-India relations and cyber events

The problem between China and India, which is essentially based on border claims, has deepened since last year with the cyberattacks by the supposedly Chinese-backed hacker group on India's critical infrastructure.

As early as last year, evidence emerged of an attempt by the Chinese government to control Indian citizens and critical infrastructure, leading to a ban on 118 Chinese apps including TikTok as 'prejudicial to [the] sovereignty and integrity of India, defence of India, security of [the] state and public order.'

'There are significant concerns over pre-positioning of network access to support China's strategic objectives.' (Security Boulevard)

An attack was carried out by China in the Galwan Valley in June last year in which more than 20 Indian soldiers were killed. Four months later, the power went out in Mumbai and life in the city of 20 million was paralysed. According to the NY Times, it is believed by the authorities that there is a link between these two events and that China is trying to put pressure on India to accede to its demands.

Recently, a US cybersecurity firm, Recorded Future claimed that Chinese-backed hacker group RedEcho attacked India's critical infrastructure last month: 'RedEcho has been seen to systematically utilise advanced cyber intrusion techniques to quietly gain a foothold in nearly a dozen critical nodes across the Indian power generation and transmission infrastructure,' said Stuart Solomon, Chief Operating Officer of Recorded Future.

It is believed that the attack was carried out by injecting malicious code into electricity generation and distribution centres. Since Recorded Future cannot access the code, a report by the Indian authorities on the incident is expected.

Following cyberattacks on the energy sector, cyberattacks continued on the transport sector and industry. The Indian national CERT has seen numerous intrusion activities by Chinese state-sponsored actors to collect intelligence and conduct cyber espionage. The actors were reportedly using either social engineering (spear-phishing), drive-by download or exploiting known vulnerabilities of public applications as an initial entry and to compromise the enterprise networks of automobile manufacturers and transport sector agencies and organisations.

There are also examples from other parts of the world, most recently from Iran where a power outage that crippled the uranium enrichment operations in Natanz was blamed on Israel. While Israel has not accepted responsibility for the attack, Israeli media claim that it was a cyberattack carried out by Mossad.

Although destructive attacks that can be attributed to state actors are rarely seen in NATO or EU nations, these examples show that countries can use their cyber capabilities as a tool of coercion to achieve political-strategic goals such as the effect on the economy, essential services or essential living needs of the population. Such behaviour is especially dangerous among such powerful countries as India and China, especially as there is no consensus in the international community on rules of conduct in cyberspace and on how cyber incidents are characterised. Therefore, it is not enough just to say that international law applies to cyberspace, but international law and norms must also be implemented. States should publicly condemn such acts, especially in the event of a cyberattack on critical infrastructure that allows the state to provide essential services.

Policymakers should be aware of the strategic consequences of cyber incidents and their role in cyberspace, especially in the use of business assets as a social layer of cyberspace. They have two roles in the contemporary security environment: to design security policy and as users of cyberspace. The same applies to NATO, the EU or any other international organisation and its officials, as they take part in setting and promoting international norms and at the same time depend on the critical infrastructure of the host countries. Therefore, all international organisations should promote trust between their member states and sharing information and promote a single information security and cybersecurity policy setting out technical and security measures (common standards) for all cyberspace entities.

Increased cyber risk due to remote working

In recent years, the number of remote workers has slowly but steadily increased. However, in March 2020 the COVID-19 pandemic forced social distancing, travel restrictions and a global effort to slow down infection rates caused a rapid shift to remote working.

Many businesses were unprepared for the overnight transition. With IT systems and security precautions often not established to allow remote working, many businesses faced greater exposure to cyber risks.

Even though the hardware and software solutions may be in place to secure the organisation's data, there were often no established policies or guidelines to help employees through the jungle of threats and vulnerabilities they were to face when moving their workplace out of the traditional office environment and into their own homes.

With a lack of appropriate guidelines, training and cybersecurity awareness, adapting to the new normal was difficult and remote workers may inadvertently have acted in ways that exposed the business to cyber threats.

Frequently reported examples of these kinds of mistakes were connecting work devices to public Wi-Fi networks, sharing corporate devices with family members without authorisation, connecting work devices to personal equipment without authorisation and using personal devices to access work applications and downloading unauthorised applications contrary to organisational policy. All of these habits increase the risk of data exposure.

A survey on the state of remote workers in 2020 showed that 45% of respondents shared their work computer with someone else in their household and 36% accessed work applications on a personal device (OneLogin).

Depending on an organisation's security policy, using corporate devices in ways that do not constitute acceptable use may put the user at risk of violating company confidentiality rules. Where employees bypass IT security by installing non-approved applications, this may introduce new vulnerabilities that are not currently within the organisation's cyber risk management programmes, resulting in increased risk exposure that is unknown to the organisation's cyber defence team.

When transitioning from an office environment to remote working, the need for connectivity and the continuation of business activity is vital. In the urgent shift in spring 2020, this focus on business continuity often takes priority over the need for confidentiality. In the longer term, employees frustrated with security constraints that limit their productivity or effectiveness may go outside the organisation's IT department processes and use personal devices, personal mail accounts and non-approved video conferencing platforms, something known as shadow IT. [6]While shadow IT can improve efficiency and productivity, it can also introduce security risks to the organisation through data leaks and compliance violations.

When establishing security policy, the leadership needs to balance the security aspects with the need to be able to complete the organisation's mission. To be able to do this they need to have full visibility of both how the implementation of security measures will affect the way people can work and the risks that result if the measures are not taken.

In cases of collaboration across organisations, availability is critical as different organisations use, for example, different solutions for video conferencing and a common platform needs to be identified, often quickly, resulting in unwanted risks for organisations as applications and services are used without proper risk management.

To transition to remote working, the tools need to be appropriate to the needs of the workforce. Dismissing employees' needs inevitably leads to them circumventing policies that appear overly restrictive or prevent them from carrying out their role. Cybersecurity is not just about technical solutions and hardening systems. Although remote workers need to be provided with the appropriate tools, hardware and software, the most important asset to address is the people. Even with strict policies and the right tools in place, employees will be able to find ways around security measures and expose the business to risk, and this must be considered.

For organisations to secure their remote workforce, the mitigating measures should start with the people. By providing needs-based cybersecurity awareness training to all employees, the organisation will equip them with the right knowledge, tools and mindset that will help them make good decisions and reduce the risk of them falling prey to cyberattacks.[7] As we have seen during the past year, opportunistic cyber-attackers are using the situation to their advantage, tailoring phishing and ransomware attacks to take advantage of the increased interest in COVID-19 related information. Training needs to be updated frequently to reflect the situation. Policies and guidelines need to keep in accord with the constant

[6] 'Shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organisation.' (Cisco).

[7] Research shows that needs-based training is more effective than blanket undifferentiated training, across organisations. For a literature overview, see *Everyday Cyber Security in Organisations*

developments and include the added risks of remote work.

Another mitigation measure that will help lower the risk of exposing business data is to implement multi-factor authentication (MFA). Requiring users to authenticate themselves by not only username and password will lower the risk of successful brute force attacks. Using MFA contributes to making the remote login process less vulnerable to cyberattacks.

If employees are required to access centralised data, make sure this is only accessed through secure communication solutions. One option is to allow access only through VPN tunnelling. By doing this, all data will pass through the organisations own security systems, but other solutions may be needed for cloud-based architectures. The compartmentalisation of data is also important so that a breach in security in one particular place or system does not expose all the company's data.

Cyber exercises for the strategic level

> **'We must also continue emphasising the need for training on strategic decision-making level. The Locked Shields also offers national senior-level decision-makers the chance to test their readiness to manage a crises' (Kaja Kallas, Prime Minister of Estonia, at Locked Shields 2021)**

National security is dependent on our ability to defend networks that support our critical functions. This is not purely a technical issue. How our national cybersecurity strategies are translated into policies and procedures needs to be understood by all stakeholders. It is important to exercise the strategic level of cybersecurity for decision-makers. Decision-making at the strategic level forms an integral part of cyber resilience and must therefore be part of exercises. Aspects of decision-making during a major cyber event include:

→ who has the authority to make which decisions;

→ how long it takes to effectuate the decisions;

→ how the information used to make the decisions should be classified;

→ how transparent the process is; and

→ whether mechanisms to share information between agencies, the private sector and partners are available.

The NATO CCDCOE annually executes Locked Shields, the largest and most complex live-fire cyber defence exercise in the world. Over the past ten years, the CCDCOE has leveraged partnerships with industry to create more complex networks including industrial control systems (ICS)/SCADA and military networks. This provides the training audience with a unique opportunity to practice how they would respond to an actual cyberattack.

Locked Shields began as a purely technical competition pitting first-rate ethical hackers against national cyber defenders. In 2017, the CCDCOE integrated a strategic decision-making element to the exercise to demonstrate the dependencies of societies on cyber-enabled infrastructure and provide a platform for nations to exercise decision-making at the political and strategic level. Cyberattacks may have an enormous impact effect on modern society and national leaders need to practice appropriate and timely responses to defend their nations. The strategic decision-making element of cyber exercises such as Locked Shields allows senior leadership the opportunity to gather stakeholders from government and private industry to discuss their roles in defence during a cyberattack. Adding a strategic element to cyber exercises also allows senior leadership to:

→ practice processes and procedures as outlined in national cyber strategies;

→ understand the coordination and decision-making process during a cyber event, both domestically and internationally; and

→ understand cyber interdependencies, not just between public and private institutions, but also among like-minded nations.

Locked Shields is a two-day exercise with the strategic decision-making element of the exercise occurring as a separate phase on the afternoon of the second day (approximately four hours). During the first part of the strategic decision-making exercise, which is conducted as a Tabletop Exercise (TTX), the training audience receives injects focused on how they would react to the cyber vulnerabilities which have been exploited during the technical part of the exercise. The second part consists of interviews where participants may practice their strategic communications in response to a cyberattack.

The target audience for the strategic decision-making exercise is ministers and senior government officials (at ministries of defence, interior, foreign affairs and finance), military and civilian CERTs and executives from key private industry.

It is always beneficial to practice the national response to a cyber crisis in an exercise environment before having to respond to an actual situation. In this light, the benefits of also conducting strategic decision-making exercises should be evident. Bluntly expressed, there is nothing to lose except the chance to get better and more resilient. Since the 'correct answers' to exercise injects depend on national cyber strategies, participation in strategic decision-making exercises is an excellent opportunity to test these strategies and make sure that all aspects are adequately covered.

The focus of cyber exercises will naturally remain on exercising the technical aspects of cybersecurity, but to create an in-depth resilience it is also necessary to exercise strategic decision-making regularly. Luckily, more and more nations seem to realise this and the appetite for strategic decision-making exercises is growing as demonstrated for instance in the latest iteration of the exercise Locked Shields which finished on 15 April.

CONTRIBUTORS

Henrik Beckvard
Emre Halisdemir
Kadri Kaska
Gry-Mona Nordli
Damjan Štrucl
Urmet Tomp
Michael Widmann
Jan Wünsche
Philippe Zotz

PREVIOUS ISSUES

This paper is part of a series of monthly reports. This issue and all previous issues are available in the CCDCOE online library.

FEEDBACK

To continuously improve this regular report, input from readers is essential. CCDCOE encourages feedback on both how the reports are of use to you and how you think they can be made better.

Please send your comments and suggestions to feedback@ccdcoe.org