VB2021
localhost

7 - 8 October, 2021 / vblocalhost.com

‘FOOL US!’, OR IS IT ‘US FOOLS!’?… 11 ‘FOOLS’ YEARS LATER…

Righard J. Zwienenberg
ESET, The Netherlands

Eddy Willems
GDATA, Belgium

righard.zwienenberg@eset.com

eddy.willems@gdata.de

ABSTRACT

Eleven years ago, in our presentation ‘Attacks from the inside…’ at the Virus Bulletin 2010 Conference in Vancouver, we outlined and provided examples of a variety of possible scenarios for internal attacks. We concluded with a top nine problems of ‘in-the-cloud services’. Now, 11 years later, we are both surprised that our predictions and warnings seem to have been completely ignored, with all of them having materialized.

In this presentation, we will ‘relive’ our 2010 presentation, while illustrating with recent examples that our message and warnings are as current and relevant now as they were then. Nothing has changed, except that internal attacks now also come from the outside.

During the COVID-19 pandemic the corporate world changed, with ‘remote working’ meaning that inside and outside became mixed. In a recent incident, eight of the top nine problems we identified 11 years ago were present, and all were foolishly ignored by professionals working from home. We considered naming the presentation ‘Attacks from the inside, by the outside…’, but as lessons learned and advice given in 2010 by ‘us fools’ seem to have been ignored, we assume that no one cares and really thinks ‘fool us!’.

We genuinely hope that the message we bring this time, combined with recent real-life examples, will not be in vain.

INTRODUCTION

Companies often forget to protect the inside of their networks against all kinds of possible attacks when there are many external entities that have access to the internal network (contractors, telecommuters, VPN connections, etc.). Moreover, even with protection in place, it is possible to fall victim to attacks from the inside. This may be a result of someone receiving a ‘legitimate’ email message with clickable content or an apparently legitimate request, for example, for information to be filled in and returned to the ISP.

SOCIAL ENGINEERING AND PRIVACY

Social engineering attacks on enterprise security systems use a combination of interpersonal skills, research and technical expertise to exploit human nature to breach corporate and personal privacy. As social engineering involves getting internal information, it can be seen as an example of an attack from the inside.

Social engineering involves the manipulation of people, rather than technology, to successfully breach an enterprise’s security model.

Despite our advances in technology, social engineering remains the single greatest security risk, and many of the most damaging security breaches are the result of social engineering, not electronic hacking or cracking. Many hacking attacks are based on social engineering.

Social engineering depends on an understanding of human behaviour, and on the ability to persuade others to release information or perform actions on the attacker’s behalf. Persuasion itself is an art and a science; studies show that humans have certain behavioural tendencies that are exploitable via careful manipulation. Some individuals possess a natural ability to manipulate, while others develop the skill through practice using positive (and negative) reinforcement. Social engineering attackers play on these tendencies and motivators to elicit certain responses in the target.

A study published in *Scientific American* in 2001 [1] cites five basic tendencies of human behaviour that help generate a positive response:

- Reciprocation: you give a freebie and want to do something with it.
- Consistency: certain behaviour patterns are consistent.
- Social validation: everybody behaves in the same way.
- Liking: people tend to say ‘yes’ to those they like.
- Scarcity: something in low supply will become precious.

Anyone or any device that stores or accesses information is vulnerable to a social engineering attack, and no person at any level of the enterprise is safe. While an old invoice or phone list may not seem dangerous in and of itself, an attacker can use this information to develop a relationship by demonstrating ‘inside’ knowledge as a way of gaining short-term trust. Electronic systems are subject to direct attack or probing. Learning a system name or IP number may allow an attacker to present themself as a network technician, and a large amount of information on your enterprise or personnel is probably available on the Internet in public or private databases. Social engineering attackers can often gain at least limited access to enterprise systems, even if it is just by looking over someone’s shoulder during an on-site visit. Every little scrap of information is valuable to an attacker.

It is important to remember that social engineering attacks are often cyclical, with attackers slowly gaining more information with each cycle until they reach their target. Information can be public or private, sensitive or non-sensitive, secure or non-secure. Unfortunately, there are large amounts of information that are public, sensitive and non-secure, such as financial data, personal data, platform details for systems and networks, and leaked secret documents. Malicious individuals have always known that the best way around any security system is to manipulate a human target into giving them what they want. It remains the single greatest security threat to enterprises. Security-aware employees, strong authentication, and effective checks and balances are the most effective methods to defend against internal and external social engineering attacks.

SOCIAL NETWORKING PROBLEMS

Social networks such as *Facebook*, *Instagram* and *TikTok* attract everybody. The intention of these sites is for users to keep in touch with existing friends, exchange information, and search for new friends. There are also many other sites, such as *LinkedIn* or *ClassMates*, used for maintaining business contacts or for searching for old school friends. Social networks are great places to meet and network with people who share similar business interests but they are also very dangerous to users and their companies. Many businesses view social networking sites as a kind of online cocktail party: a friendly, comfortable place where one can establish contacts, find buyers or sellers, and raise a personal or corporate profile.

However, the cocktail party metaphor is not entirely accurate. In fact, users would be better served if they thought of social network services as a loud glass house: a place with endless visibility and each occupant talking through a highly amplified horn. Since most people access social network sites from the comfort and privacy of their home or office, they can be lulled into a false sense of anonymity. Additionally, the lack of physical contact on social network sites can lower users’ natural defences, leading individuals into disclosing business or private information they would never think of revealing to a person they had just met on the street or at a cocktail party.

Over-sharing company activities

When someone gets excited about something his or her company is working on and simply must tell everyone about it, a problem arises. By sharing too much about your employer’s intellectual property, you threaten to put them out of business by tipping off a competitor who could then find a way to duplicate the effort or to spoil what they cannot have by hiring a hacker to penetrate the network. Then there are hackers controlling botnets that could be programmed to scour a company’s defences and, upon finding a weakness, exploit it to access data relating to intellectual property. With the data in hand, the hacker can then sell what they have to the highest bidder, which just might be your biggest competitor. Sharing this kind of information could lead to targeted attacks on specific technology-producing enterprises.

Mixing personal with professional

This problem is closely related to the first, but extends beyond the mere disclosure of company data. This is the case where someone uses a social network for both business and pleasure, most commonly on *Facebook* and *Instagram*, where one’s ‘friends’ include business associates, family members and actual friends. The problem is that the language and images one shares with friends and family may be entirely inappropriate on the professional side. A prospective employer may choose to skip to the next candidate after seeing pictures of you drunk or showing off at someone’s birthday party. In sharing such things, you also stand a good chance of making the company you represent look bad. In some cases, it is nearly impossible to separate the business from the personal on a social networking site. Those who work for media companies, for example, are sometimes required to use all their social networking portals to proliferate content in an effort to boost page views which, in turn, attracts potential advertisers. But wherever and whenever possible, security practitioners work to keep people locked in their respective boxes.

Most connections?

For some social networkers, it is all about accumulating as many connections as possible. Folks on *LinkedIn* are notorious for doing this, especially those in some specific *LinkedIn* groups. This may seem harmless enough or, at the worst, just annoying. However, when the name of the game is quantity over quality, it is easy to link with or accept a ‘friend’ request from a scam artist, terrorist or identity thief.

Clicking on everything

Facebook and *Twitter* in particular are notorious as places where inboxes are stuffed with everything from drink requests to invites to join a cause. For some social networkers, clicking on such requests is as natural as breathing. Unfortunately, the bad guys know this and will send links that appear to be from legitimate friends. Open the link and you are inviting a piece of malware to infest your machine.

Endangering yourself and others

Reckless social networking can literally put someone’s life in danger. It could be a relative or co-worker. Alternatively, it could be you. It is advisable and logical to pay extreme caution when posting birthday information, too much detail on your spouse and children, etc. Otherwise, they could become the target of an identity thief, be used to break the security question on one of your services’ password reset forms, etc.

TODAY'S NETWORKS LACK CLEAR, CRISP BOUNDARIES

Where does the boundary of either a private or a business network end these days? This is not so easy to define anymore. In the past several of us could work easily from home through a secured VPN connection; in current times, with enforced remote working, most people have to work from home, and that is where companies are opening up parts of the network to the outside world. Employees are logging into their companies' email systems in open public places to check their email. It is obvious, of course, that password stealers and other spyware could easily be used to reveal the login and password details, giving any hacker access to inside information from the company. Other problems come increasingly from mobile devices, on which email checking is routine these days, but which can even be used to log into a remote desktop. If used on a public network, it could easily be sniffed to reveal the login details to the hacker who is drinking a cappuccino in the same coffee shop as you are checking your mail. Most of us have good protection in place at home but many people do not think about these possible problems in public places. As today's networks lack clear, crisp boundaries, it becomes more and more difficult to define the real inside and outside of the corporate network. It even becomes more and more difficult for typical users to protect themselves and to detect the real risks behind every part of the network. This issue is likely to increase and will become more and more problematic in the coming (yet another 11?) years.

Network segments, both internal and external, are now so interconnected that any kind of incursion will spread throughout the network; any kind of trojan enumerating the network for open shares will find them, etc. Over the years, most malware attacking corporate intranets has spread over three well-known protocols: CIFS, SMB and RPC.

THE CLOUD

Working definition of cloud computing

This is the working definition of cloud computing we are using for the purposes of this article. It is not intended as yet another definitive definition [2]:

> *Cloud computing is an on-demand service model for IT provisioning, often based on virtualization and distributed computing technologies. Cloud computing architectures have highly abstracted resources, near instant scalability and flexibility, near instantaneous provisioning, shared resources (hardware, database, memory, etc), 'service on demand', usually with a 'pay as you go' billing system, programmatic management.*
>
> *Cloud computing is an on-demand service model for IT provision, often based on virtualization and distributed computing technologies. Cloud computing architectures have:*
>
> - *highly abstracted resources*
> - *near instant scalability and flexibility*
> - *near instantaneous provisioning*
> - *shared resources (hardware, database, memory, etc)*
> - *'service on demand', usually with a 'pay as you go' billing system*
> - *programmatic management […]*
>
> *There are three categories of cloud computing:*
>
> - *Software as a Service (SaaS): is software offered by a third party provider, available on demand, usually via the Internet and remotely configurable. Examples include online word processing and spreadsheet tools, CRM services, and web content delivery services (Google Docs, Office365, Box, etc.).*
> - *Platform as a Service (PaaS): allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms. (Microsoft Azure, Google App engine, etc.).*
> - *Infrastructure as a Service (IaaS): provides virtual machines and other abstracted hardware and operating systems, which may be controlled through a service API. (Amazon AWS, Oracle Cloud, Windows OneDrive, Rackspace Cloud, etc.).*

SECURITY BENEFITS OF CLOUD COMPUTING

The security benefits of cloud computing include:

- The benefits of scale and rapid, smart scaling of resources
- Standardized interfaces for managed security services
- Audit and evidence gathering
- More timely, effective, and efficient updates and defaults.

TOP #11 'IN-THE-CLOUD' PROBLEMS

It is hardly necessary to repeat the extensive material that has been written on the economic, technical, architectural and ecological benefits of cloud computing. An examination of the security problems related to cloud computing, as has recently been reported in news from the 'real world', must be balanced by a review of its specific security benefits. Cloud computing has significant potential to improve security and resilience; however, special care must be taken with regard to several upcoming threats. We will try to give you an overview of the most important 'in-the-cloud' problems [3].

#11 Identity management

You can never be sure who is really is who. Attackers can misuse your identity. The cloud does not really know who you (physically) are. If attackers can gain access to your network, they can communicate with the cloud. Because the cloud thinks it is still communicating with a trusted source (your network), lots of information can be intercepted/stolen or the cloud can be fed with lots of faulty data.

Another possibility is an identity management man-in-the-middle attack where the attacker is between the network (victim) and the cloud.

#10 Nefarious use of service

Providers offer their customers the illusion of unlimited computing, network, and storage capacity – often coupled with an easy registration process where anyone with a valid credit card can register and immediately begin using cloud services. Some of them even offer free trials. By abusing the relative anonymity behind these registration and usage models, criminals have been able to conduct their activities, sometimes without any interference. Current and future areas of concern include password and key cracking, DDoS, launching dynamic attack points, hosting malicious data, botnet command-and-control centres, cryptocurrency mining and CAPTCHA-solving farms.

Good old examples of this problem are the service providers that have hosted the Zeus botnet and downloads of exploits for *Microsoft Office*, *Adobe* PDF, etc. Additionally, botnets have used IaaS servers for command-and-control functions. Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud computing providers are actively being targeted because their easy and weak registration systems facilitate anonymity and because providers' fraud detection capabilities are limited [4].

DDoS attacks are also a very good example of this, as they have become a trend over the past few years. Approximately 2.9 million DDoS attacks were launched in the first quarter of 2021, according to research from *Netscout*'s ATLAS Security Engineering & Response Team (ASERT). The estimated figure represents a 31% increase compared to the same period in 2020. All three months of the year's first quarter saw more than 900,000 DDoS attacks, which researchers said exceeded the existing baseline of 800,000 per month. At the end of 2020, *Google*'s cloud business disclosed an incident that had involved bombarding the company's Internet networks with a flood of traffic. The DDoS attack lasted over a six-month campaign, peaking to 2.5 Tbps in traffic. The attackers used several networks to spoof 167 Mbps to 180,000 exposed CLDAP, DNS and SMTP servers, which would then send large responses back to the *Google* servers. This was four times larger than the previous high of 623 Gbps from an attack via the Mirai botnet a year earlier. These examples clearly show that nefarious use of service is a hard problem to tackle and possibly will grow along with the growth of bandwidth internationally.

#9 Account/service hijacking

If a cloud account or service is hijacked one way or another, it can be misused for almost any kind of malicious intent, depending on the original service provided. Whenever this happens, it can have very nasty consequences for both the users and the companies that are hit. Eventually, the owner of the account will be blamed. A classic example of this is the (in)famous Twittergate of 2009. A more recent example – also involving *Twitter* – was celebrities 'giving back to my community due to Covid19!', where people were promised that all bitcoins sent to the celebrity's wallet would be returned doubled, but only for the next 30 minutes.

#8 Financial DDoS

In several different scenarios, other parties may use a cloud customer's resources in a malicious way that has a financial impact:

- Identity theft: attackers use an account and use the customer's resources for their own gains or in order to damage the customer economically.
- Unexpected loads on resources: if the cloud customer has not set effective limits on the use of paid resources, they may experience unexpected loads on these resources through malicious actions.
- Use of metered resources: an attacker uses a public channel to use up the customer's metered resources – for example, where the customer pays per HTTP request; a DDoS attack can have this effect.

A financial DDoS destroys economic resources; the worst-case scenario would be a serious economic impact or the bankruptcy of the customer.

Even phishing attacks are examples of this as they can put families or individuals at high risk. A good example of this is the case of Belgian citizen Danny Hoedemaekers, who got phished for a sum of EUR43,000 (all of his money; approximately US$52,000) in one night in 2020. It resulted in a crowdfunding campaign to replace the lost money. A Belgian artist created a charity auction to help the victim as well [5]. The bank involved had not set effective limits (e.g. amount of money, time limits, etc.) to stop these kinds of threats.

#7 Data loss/data leakage

Imagine a document containing classified information being stored or being scanned in the cloud. Who is behind the cloud? Everything that happens *within* your company can be controlled – you control what goes out, but what happens when it gets to the cloud? Is it forwarded automatically to 'someone' or 'something' else? If it is scanned (for malware) in the cloud and is misidentified (a false positive), will it be quarantined in the cloud? Due to legislation issues, besides the issue of being quarantined (or worse: deleted), where is it stored? We will come back to that later.

We hear more and more about data breaches and the data lost. Over the years, they have occurred with increasing frequency, which is nicely represented by *Information is Beautiful* [6]. With a world more digitized than ever, breaches and thus data loss will naturally occur more. However, since 2016, it looks like the growth in breaches and data loss is exponential. Is it? Perhaps, but it is most likely that the GDPR legislation [7], and the heavy fines involved when not reporting a data breach, had a 'positive' effect on the total number of breaches publicly reported.

#6 Unknown risk profile

One of the advantages of cloud computing is the reduction in hardware and software ownership and maintenance required, allowing companies to focus on their core business strengths. This has clear financial and operational benefits, which must be weighed carefully against security concerns. Versions of software, code updates, security practices, vulnerability profiles, intrusion attempts and security design, are all important factors for estimating your company's security position. Information about who is sharing your infrastructure may be pertinent, in addition to network intrusion logs, redirection attempts and/or successes, and other logs. Security by obscurity may be low effort, but it can result in unknown exposure. It may also impair the in-depth analysis required in highly controlled or regulated operational areas.

When adopting a cloud service, the features and functionality may be well displayed, but what about details or compliance of internal security procedures, configuration hardening and patching? How are your data and related logs stored and who has access to them? What information, if any, will the vendor disclose in the event of a security incident? Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile.

A clear and old example of this problem is the *Heartland* data breach: *Heartland*'s payment processing systems were using unpatched software known to be vulnerable to attack. And *Heartland* was 'willing to do only the bare minimum and comply with state laws instead of taking the extra effort to notify every single customer, regardless of law, about whether their data [had] been stolen.' [8]

Other more recent examples are the *Facebook* and *LinkedIn* data breaches from 2021 where, in both cases, personal details of over 500 million users had been publicly available in unsecured databases. The *Facebook* hack was deeper (more personal details, such as phone numbers and addresses) compared to the *LinkedIn* attack, but in both cases, data was scraped through the web interfaces. *Facebook* and *LinkedIn* claimed to have performed the necessary steps to prevent this; however, the breaches clearly showed that was not enough. Users' data can be misused in future phishing and spear-phishing attacks.

#5 Hidden logs/intrusion attempts

A direct attack aimed at a company's network will be noted and is visible in the gateway log files. However, what if the attack is aimed at the cloud? Attackers could forward all messages to themselves; none of this gets noticed in the company's gateway log files!

#4 Insider abuse

Insider abuse can be a lot more dangerous than outsider abuse. While an outside attacker needs to work to find an external attack vector into your networks and physical facilities, insiders already have authorized access to your buildings and user accounts, so an insider can usually skip these initial steps. It is a lot easier to privilege escalate from a user account you already have than to break into any user account in the first place. Security guards will scrutinize an unfamiliar individual, whereas they will wave 'hello' at a known employee. The same applies to accidental incidents. It is not easy to know any sensitive information about companies that you have never worked for. A current or former employee often does know such information, and it may be socially engineered out of them.

The malicious activities of an insider could potentially have an impact on the confidentiality, integrity and availability of all kinds of data, IP and services, and therefore indirectly on the organization's reputation, customer trust and the experiences of employees. This can be considered especially important in the case of cloud computing because cloud architectures necessitate certain employee roles that are extremely high risk. Examples of such roles include system administrators and auditors and managed security service providers dealing with intrusion detection reports and incident responses.

As cloud use increases, employees of cloud providers increasingly become targets for the cybercrime community. For in-the-cloud companies, insider abuse carries more risks than for businesses that are still more in the 'on-premises' camp, as the impact could be much wider and target several companies instead of one in particular. The vulnerabilities here are clear and range from unclear roles, system or OS vulnerabilities, and inadequate physical security procedures to application problems or even poor patch management. To complicate matters, there is often little or no visibility regarding the hiring standards and practices for cloud employees. It is clear that the level of access granted could enable a criminal to harvest confidential data or to gain complete control over the cloud services with little or no risk of detection. It is also clear that several problems like these are mostly not conveyed to the public, as this could have too large a financial impact on the 'in-the-cloud' service provider [9].

A possible example of this: in 2019 it was reported that an Iranian mole working for Dutch intelligence at the behest of Israel and the CIA inserted the Stuxnet worm [10] with a USB flash drive or convinced another person working at the Natanz facility to do so. Insiders are always more trusted, and intelligence services know this pretty well.

#3 Centralized AAA abuse/trust

Authentication, authorization and accounting (AAA) [11] is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. If the AAA cannot be guaranteed, e.g. if an account is hijacked, any actions taken by the malefactor will be put on the holder's account and all 'trust' on their name.

#2 Supply-chain attacks

Wikipedia describes a supply-chain attack [12] as 'a cyberattack that damages an organization by targeting less-secure elements in the supply chain'. A supply-chain attack can occur in any industry or domain. A supply chain is a system of activities involved in handling, distributing, manufacturing and processing goods in order to move resources from a vendor into the hands of the final consumer. A supply chain is a complex network of interconnected players governed by supply and demand. Generally, a supply-chain attack on information systems begins with a threat actor that determines a member of the supply network with the weakest cybersecurity in order to affect the target organization.

Supply-chain attacks pose significant risks to modern organizations, and attacks are not completely limited to the information technology sector; supply-chain attacks affect every kind of industry ranging from the oil industry and large retailers to the pharmaceutical sector and nearly any industry with a complex supply network. In many cases, poorly managed supply-chain systems can become significant targets for cyber attacks, which can lead to loss of sensitive customer information and disruption of the manufacturing process. It could damage several companies', or organizations', reputations completely and simultaneously.

For example, we might think of the SolarWinds exploit (December 2020). Here, the attackers used a typical supply-chain attack. The attackers accessed the build system of the software company *SolarWinds* [13]. In the build system, the attackers modified software updates provided by *SolarWinds* to users of its network-monitoring software *Orion*. In March 2020, the attackers began to plant their remote access malware into *Orion* updates. Their potential victims included US government customers in the executive branch, the military and the intelligence services. Afterwards, several other federal departments were found to have been breached. Even where data was not exfiltrated, the impact was significant in the whole supply chain.

A very important aspect of a supply-chain attack is that it endangers a whole series of other companies and organizations within the attack by disrupting typical services or the supply chain itself.

Another example of this is the Colonial Pipeline attack in the US (May 2021) [14] where a ransomware attack led one of the largest US fuel pipeline operators to shut down its entire network. The shutdown itself had an immediate impact on fuel delivery and caused a cascade of dramatic impacts, including higher prices and consumer hoarding of gasoline. Without corrective measures, this could have posed a pipeline integrity risk to public safety, property or the environment. The supply chain is quite huge in this case.

#1 GDPR vs. Cloud Act issues

What you store, and where, matters! Even though in 2016 the EU and the US signed the Privacy Shield treaty [15], which should guarantee the privacy of European citizens, recently, the EU Court clarified for a second time that there is a clash between EU privacy law and US surveillance law [16]. As the EU will not change the fundamental privacy rights of its citizens to please the NSA, the only way to overcome this clash is for the US to introduce solid privacy rights for all people – including for non-US citizens.

The story is more complex than pictured here, but not as negative as many people think. Larger companies like *Microsoft*, *Amazon* and *Google* store data of European companies in Europe. Those European branches fulfil (mostly) the EU GDPR regulations as their data storage is disconnected from the parent company. However, takeovers are a problem. A 100% European provider can be acquired or taken over by a US company and then right away is submitted to US legislation, according to the US. As a business entity, you can take precautions and protect yourself by storing all data encrypted, to comply at least with GDPR. That is for now! One never knows how the cloud and local laws around privacy will evolve.

CONCLUSION

No matter how hard you try, from the inside, to protect your networks from attacks emanating from both within and without, there are still plenty of ways in which these attacks can occur. Unknown third parties or services with unknown risk profiles, rogue employees and social engineering are all things that can and actually do take place in attacks on your network or in the cloud – attacks starting from the inside or from the outside. In many cases, the human aspect is the underestimated part. This top 11 of very important in-the-cloud cyber threats shows that the situation is not improving at all. On the contrary, some of the threats that we outlined back in 2010 have even become trends in 2021. This illustrates that many more security measures need to be taken to counter existing and possible new trends and ever more sophisticated cyber attacks. Let us hope this will change in the next 11 years. The future will tell.

REFERENCES

[1] Cialdini, R. B. The Science of Persuasion. Scientific American. February 2001. https://www.scientificamerican.com/magazine/sa/2001/02-01/.

[2] ENISA. Cloud Computing: Benefits, risks and recommendations for information security. ENISA white paper, Rev.B December 2012. https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security.

[3] Cloud Security Alliance. http://www.cloudsecurityalliance.org/.

[4] Wikipedia. Zeus (malware). https://en.wikipedia.org/wiki/Zeus_(malware).

[5] De Rijke, J. Internetfraude piekt: klachten over phishing verdubbeld in coronajaar 2020. Knack. https://www.knack.be/nieuws/belgie/internetfraude-piekt-klachten-over-phishing-verdubbeld-in-coronajaar-2020/article-longread-1695677.html.

[6] World's Biggest Data Breaches & Hacks. Information is Beautiful. https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[7] General Data Protection Regulation. https://gdpr-info.eu/.

[8] Slattery, B. Heartland Has No Heart for Violated Customers. PC World. https://www.pcworld.com/article/158038/heartland_customers.html.

[9] Parry, R. An Assessment of the Risk of Service Supplier Bankruptcies as a Cybersecurity Threat. IntechOpen. https://www.intechopen.com/online-first/an-assessment-of-the-risk-of-service-supplier-bankruptcies-as-a-cybersecurity-threat.

[10] Bob, Y. J. Secret Dutch mole aided Stuxnet attack on Iran's nuke program – report. The Jerusalem Post. https://www.jpost.com/Middle-East/Secret-Dutch-mole-aided-Stuxnet-attack-on-Irans-nuke-program-report-600430.

[11] Wikipedia. AAA (computer security). https://en.wikipedia.org/wiki/AAA_(computer_security).

[12] Wikipedia. Supply chain attack. https://en.wikipedia.org/wiki/Supply_chain_attack.

[13] Wikipedia. 2020 United States federal government data breach. https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach#SolarWinds_exploit_2.

[14] Neuman, S. What We Know About The Ransomware Attack On A Critical U.S. Pipeline. NPR. https://www.npr.org/2021/05/10/995405459/what-we-know-about-the-ransomware-attack-on-a-critical-u-s-pipeline?t=1622465109530.

[15] European Commission. EU-US data transfers. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

[16] Roche, D. EU-US in collision course on privacy. Euractiv. https://www.euractiv.com/section/data-protection/opinion/eu-us-in-collision-course-on-privacy/.