Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

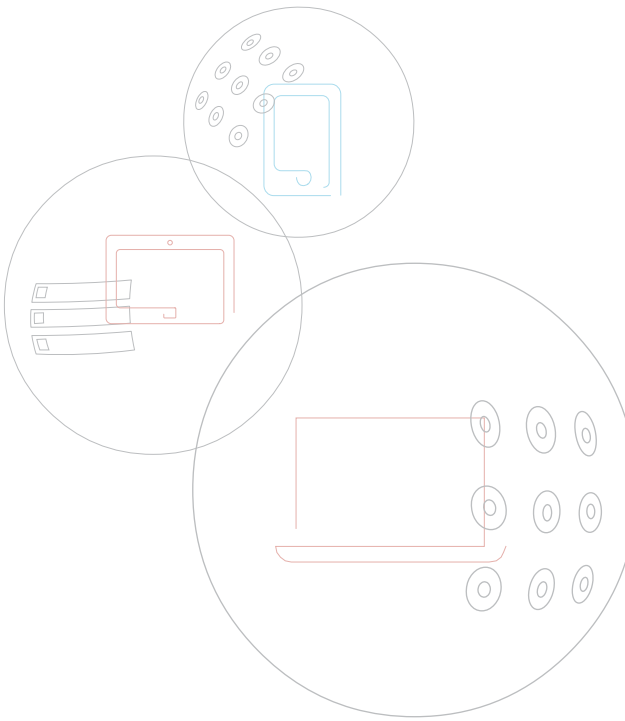
Capgemini Consulting

Trends in Cybersecurity 2016-17

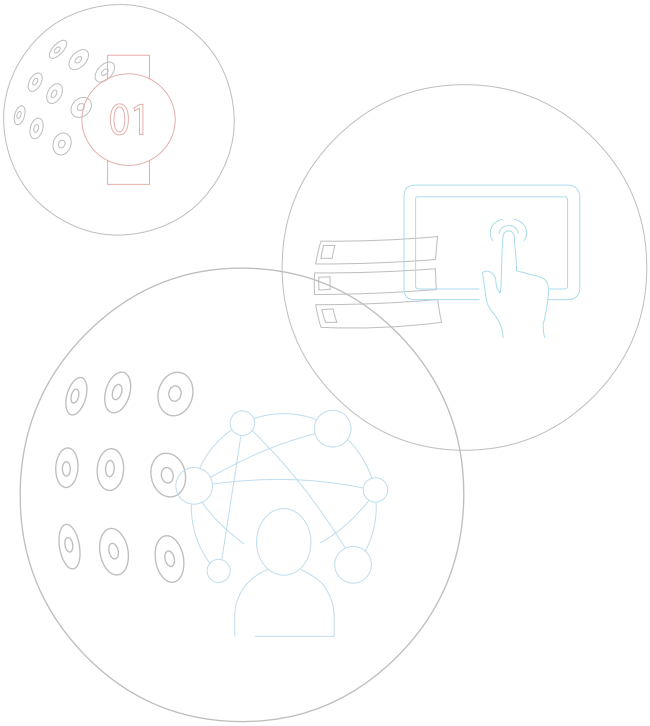
People and digital security

Trends in Cybersecurity 2016-17

People and digital security




Check-in
Economy
7
Departures
Vertrek
1
5
6



Preface

As the ancient Chinese philosophers said, every new development also has the seed of an opposite development. In these modern times, this saying may easily be applied to security and privacy. The opportunities arising from digitalization have not yet been exhausted. Think about biometrics, quantum computers and virtual reality. However, these new technologies also introduce new vulnerabilities like network risks, loss of privacy, and ultimately the decline of trust in the digital society. We see that too many organizations and individuals are just focusing on the opportunities and neglect to see the vulnerabilities.

The awareness of how organizations deal with personal data is very low among Dutch citizens. To protect them against this lack of awareness, the government has implemented stricter legislation and regulations. The Mandatory Data Breach Notification and the General Data Protection Regulation (GDPR) are examples of this. The Cybercrime III Bill also helps by offering investigative agencies more options for digital investigations.

How do you deal with these new trends? We hope the articles in this report will provide you with concrete guidelines to answer that question.

Content table



Management summary

Digitalization changes society. Driven by the wishes of the customers and citizens, public and private organizations are transforming at a high pace, in turn affecting the security domain. The articles in this report focus on several aspects of the threats for self-reliant citizens, for victims, and for professional service providers.

Seventy-five percent of the Dutch population is aware of Internet crime[1]. This is a seven percent increase compared to last year, which makes one confident that the citizens are resilient in the digital society. After all, every form of behavioral change begins with awareness; and public awareness is raised when security incidents are announced in the media.

Awareness regarding privacy matters turns out to be quite low. Only 31% of the Dutch population pays attention to whether the application requires private information, when installing any app. The choice is mainly motivated by its cost. In exchange for using a free app, users are asked to give access to their personal data, which makes privacy a means of exchange and payment. Many users are not aware of how much data an app has access to when accepting the terms of agreement.

[1]A research for Capgemini conducted by TNS NIPO among Dutch citizens on their opinions and perceptions of public order and security.

Three in ten Dutch citizens think there is a great chance that they will become victims of a cyber attack especially by means of phishing, viruses or malware infections. There is less fear for identity fraud, hacking, and ransomware. Seven in ten respondents have received an email that they didn't trust and 0.4% have transferred money to a fake account. Most Dutch citizens have between three and nine passwords, and only one third use more than ten passwords.

Internet detectives have limited legal options for collecting digital evidence and investigating suspects. The Cybercrime III Bill is still controversial, but it gives the police greater leeway to access computers of suspects. This bill is an adequate response to the wishes of the majority of the Dutch population: 89% of the Dutch think that the government should be more active against cybercrime and 81% support the additional authorization to back-hack into the computers of the suspects.

Technological advancements such as encryption do not only offer governmental agencies and citizens the opportunities to tighten security in the fight against cybercrime; criminals and unfriendly governmental agencies embrace the same technological advancements too. The arrival of quantum computers and the "Internet of Things" has accelerated this rat race. The Internet of Things (IoT) comprises of sensors, connected to physical objects, which send information and reports about themselves.

The use of biometrics as a means for authentication brings along new dilemmas. Unique biometric characteristics such as finger prints, voice, iris of the eye, or DNA are used at an increasing rate to grant users with access to a service. A good example would be the new smartphones, which require users to provide a fingerprint to unlock it, instead of typing in an access code. The use of this approach is very easy, one no longer needs to constantly remember or change their passwords or codes anymore. However, the unique physical characteristics are stored in the device for the sake of this access, and therein lies the danger. Stolen passwords can be changed quickly, but you cannot replace a fingerprint.

Even with technological advancements such as quantum computers and biometric applications, people continue to be the weakest link in the chain. It is easy to persuade people. They exhibit pre-programmed behavior that criminals know how to capitalize on; for example, by using phishing emails through USB sticks that are left behind or through "evil twin" WiFi hotspots. The risks for these types of social engineering can be reduced by practicing with them. An example would be the use of a social engineering assessment wherein a trained social engineer is commissioned to attempt to steal as much sensitive information as possible. Communication about the results to the victims afterwards helps to greatly raise one's awareness.

So what happens if it goes wrong? In any case, it is then a matter of limiting the damage and maintaining trust. Communication to those involved is crucial. Who is going to communicate with whom, what is the minimum that must be conveyed, when and through which channels? This is certainly important for organizations in the security domain because they usually work with sensitive data and trust is the basis for their legitimacy.

Cybersecurity should also be a standard component of mainstream security processes in companies. Organizations with critical infrastructure have to make digital security part of their operational processes. The Chief Information Security Officer (CISO) plays a significant role in that. The constant new streams of digital threats and the changing legislation are changing the CISO's role. These CISOs will have to let go of their traditional focus on IT so that they can better manage the constant fluctuating balance between business (where money is earned) and IT security: each of which needs the other. To prevent security from being regarded as an obstacle, however, the CISO needs legal skills along with technical knowledge.

For more information, you can contact the authors at:
erik.hoorweg@capgemini.com and matthijs.ros@capgemini.com

Privacy as means of exchange: Unavoidable, but acceptable?

What is our view of the balance between the use of apps and users' privacy?

Users are often oblivious to the quantity of personal data they are releasing when installing an app.

Highlights

- The requirements for the processing of personal data are clear.
- By accepting an application's terms and conditions, the user releases his or her personal data.
- Users are oblivious to the quantity of personal data they are releasing upon installation.
- The elements of risk management help to increase awareness about the risks and measures that can be taken.
- Users, application developers, and the government have a shared responsibility to create this awareness.

Privacy as means of exchange: unavoidable, but acceptable?

Our life increasingly centers on access to information and services, at any moment and from wherever we are. Applications (apps) on smartphones play an important role in this. In exchange for use, many apps request access to the user's personal data. Users are often unaware of the quantity of data they release when installing an app. The risk that these data may be abused is always lurking. The identification, estimation, and assessment of risks by users and the management and monitoring of these risks by the government can be a (conscious) step in the right direction.

The use of a smartphone has become standard

As of 2013, more people in the Netherlands own a smartphone than a desktop computer[1].The smartphone has become a permanent fixture in our day-to-day lives. Users want to be able to look up information, buy products, and communicate with others at any time, from any place. Apps facilitate this: a smartphone usually has an average of twenty apps installed[2].

Requirements for the processing of personal data by apps

Personal data processing encompasses all actions relating to those personal data, such as collection, recording, sorting, and consulting. In the Netherlands, the Personal Data Protection Act (Wbp) protects the user by stipulating requirements for the processing of personal data by an app:

Purpose: Personal data may only be processed for a specific purpose. These purposes must be disclosed to the user clearly and in an orderly manner prior to the data processing.

Explicit consent: The data subject must have given his explicit consent for the processing of personal data. This means that the consent has been given freely, by an informed data subject, in an active expression of will. "Given freely" refers to the fact that the data subject does not feel any pressure to consent to the processing. "Informed" means that the data subject must know what data are being processed and how this processing is taking place. An "active expression of will" must be aimed at giving consent.

The new European privacy regulation (the General Data Protection Regulation) due to take effect in 2016, stipulates even stricter requirements on informing the customer, including the period of which personal data may be kept and the right to inspect and have data deleted.

If something is free, you're the product

Apps can request access to various functions of a telephone and personal data, such as location details, photos, contacts, the microphone, or messages. Apps are usually free to install. The consumer pays for this by making his or her personal data available.

Personal data can be very valuable to businesses for numerous reasons:

- The data can help businesses improve their service[3].
- The data can be sold to advertisers or marketing companies to target the user with tailored advertisements[4].
- Other companies can secure direct access to the smartphone and abstract data.
- For example, Facebook earns € 3.39 per quarter per user by offering personal advertisements or by monitoring your internet browsing outside of Facebook[5].

Releasing personal data via apps entails significant risks

As stated earlier, the Wbp requires a free and informed consent. People are often oblivious of the nature and quantity of personal data that are released via an app, however, and how the data might be abused. Even without active use of the app, location details can be used to figure out when you are on vacation[6] : precisely the kind of information that is useful to a burglar. Credit card details filled in previously are very appealing for abuse in identity fraud.

Releasing these data and in doing so "paying" for an app with personal data entails, a certain risk for the user. Which could have a significant impact on the user's privacy. As part of its vision report Trends in Security, Capgemini had TNS NIPO carry out a survey among Dutch citizens in 2016. This indicated that almost 70% of the respondents believed that releasing personal data to apps has an influence on the commission of crime involving the abuse of data. More than half of the respondents believed that developers do not treat the data securely.

At the same time, 70% felt it was above all important that the app could be used free of charge. The average user hardly takes the time to protect his or her privacy: the results from the same TNS NIPO survey indicate that only one third of respondents read the privacy policy before deciding whether or not to install an app.

So is the average user taking a conscious risk?

It appears as if the user is making a carefully informed choice: free use and convenience prevail over concerns about the risks. The results show, however, that many users do not realize well enough what access to personal data that they give away by using apps. An example is WhatsApp, an app that eighty percent of the respondents in the TNS NIPO survey had installed. WhatsApp requests access to, among other things, the telephone's camera, microphone, location, and contacts. By accepting the terms and conditions of use, the user grants this access. One quarter of the respondents thought that WhatsApp did not have access to the contacts on their phone, seventy percent did not think that WhatsApp had access to the microphone, and sixty percent thought that the app did not have access to the camera. One in ten even thought that WhatsApp had no access at all to any of the above data.

It is clear that users are often not adequately aware of what they release by accepting the terms and conditions of use. This puts the freely-given and informed consent required by the Wbp under pressure. An important question in that case is: how far does the responsibility of the individual user reach? Can the principles of risk management help find an acceptable balance between giving away information and the risks to people's digital security?

[1] Tweakers.net: GfK: more smartphone users than PC owners in the Netherlands.
[2] Motivaction and Telecom Paper, June 2015
[3] European Data Protection Supervisor, in March 2014: Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy.
[4] Rijksoverheid.nl, 2012: Stimulating and inhibiting factors of Privacy by Design in the Netherlands.
[5] NRC Next, 1-03-2016: The product is you.
[6] Elsevier, number 4, 2016: What now Privacy?; Consuwijzer.nl: Each app has a price. Part you just data?; Kreuger, in June 2015, Your app signature is more distinctive than your DNA.

Identifying risks by creating awareness

It is the user's responsibility to treat his or her personal data carefully. Lengthy, unclear, and complex privacy statements and the lack of a clear description of the purpose for collecting data do not make it easy for users to take on this responsibility. The first step in risk management is identifying risks, which must be preceded by knowledge of the risks. The TNS NIPO survey shows that the Dutch public feels people's knowledge about the privacy risks of apps needs to be increased. The government can play a role in this, because it has for years already held a crucial role in informing consumers about risks to their (digital) security. Although 38% of the respondents indicated that they needed information from the government, the survey also showed that the developer (48%), the internet (38%), and fellow users (36%) are other sources from which respondents would like information. There is, therefore, a need for different information sources and that means there is shared responsibility among all these parties for increasing awareness among users of the privacy risks in using apps.

Figure 1: To what extent do you agree with the following assertions? (as a %)

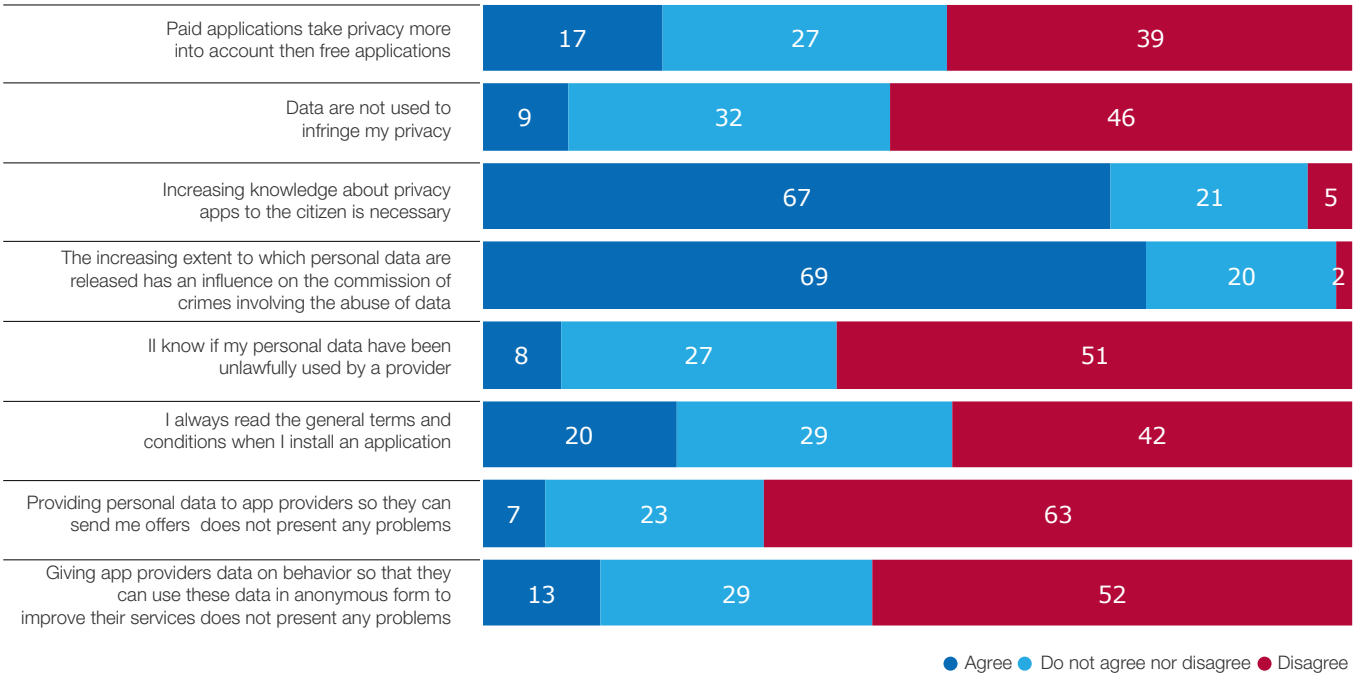
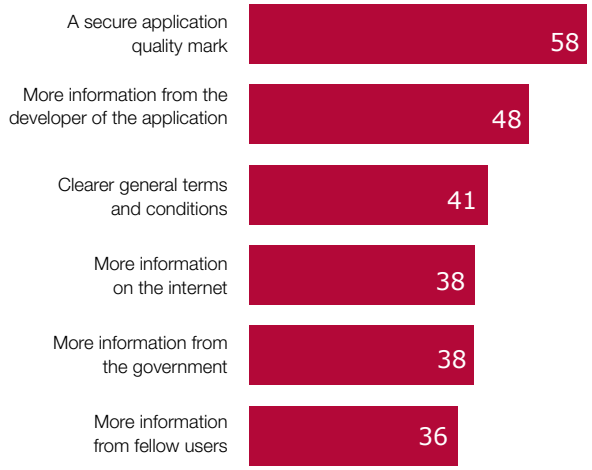


Figure 2: What would help you to be more aware what is happening with your data when installing an application?



Assessing the risks

The job of assessing the risks remains primarily with the user. Providers of apps must give users guidance in this by indicating clearly and unequivocally in their privacy statement as to what data they are requesting access to and to which third parties these data are passed on. The TNS NIPO survey indicated that 58% of the respondents see the need for a “safe app quality mark”. This kind of quality mark can show what apps have clear and unambiguous privacy statements and treat personal data securely. The Dutch Data Protection Authority could play a role in setting up and issuing this quality mark. These two elements can better enable users to assess the risks of using an app and weigh these risks against the convenience of using the app.

Managing and monitoring: a single reporting center for abuse

Two important next steps in risk management are managing and monitoring. Managing risks encompasses two aspects: precautions and responses. At the moment, there are few precautions that a user can take to protect his or her personal data and still make use of an app.

Failing to accept the terms and conditions generally means that the app cannot be used, and because of the increasingly prominent role of apps in our day-to-day lives, this is often not acceptable. Expanding the range of options for users to intervene would be a welcome development towards protecting privacy. One of the possibilities for this expansion is setting up a single reporting center for abuse. This reporting center could serve as a place where users, the government, and developers can jointly provide information, give signals, and take action.

The Dutch Data Protection Authority must also take on its role in monitoring the lawful securing of user consent (free, informed and an active act). Developers who do not treat personal data in the desired manner must also be actually adressed on this.

An acceptable balance is a communal responsibility

In summary, it can be said that it is impossible to imagine a digital society that does not include smartphones and apps. The privacy of users is currently not adequately guaranteed. Users usually pay by giving access to their personal data. Privacy as a means of exchange is most likely unavoidable, but an acceptable balance needs to be found. The principles of risk management show that this is a joint responsibility for the government, application developers, and users.

About the authors

Eva Miltenburg, MSc, is a managing consultant at Capgemini Consulting. Eva focuses on organizational issues relating to policy realization and chain cooperation in the security domain. Josca Smallenbroek, MSc, is a consultant at Capgemini Consulting. She focuses on processes, process improvement, and organizational issues in the public sector. Martine Middelveld MSc is a security and privacy consultant at Capgemini Consulting. She specializes in solving privacy issues and specifically in how organizations can set up compliance with the requirement to report data breaches.

For more information, you can contact the authors at:
eva.miltenburg@capgemini.com, josca.smallenbroek@capgemini.com and martine.middelveld@capgemini.com

Legal dilemmas in digital investigation

What legal dilemmas do digital and internet detectives face when it comes to digital investigation in criminal cases?

Digital and internet detectives currently have limited legal possibilities for collecting evidence digitally and tracking down suspects.

Highlights

- Detectives may not log into accounts using passwords they have found or acquired through wiretapping.
- Whether victims' social media may be examined with the permission of relatives is legally debatable.
- The act on Special Investigative Police Powers (abbreviated in Dutch as BOB) often falls short.

Legislative proposal on Computer Crime III:

- Police will be able to break into servers, even if these are located abroad.
- Use of "undercover adolescents" as "bait" (adults posing as adolescents).
- Online commercial fraud will become criminal law instead of civil law.
- The unlawful (re)selling of computer data will become an independent criminal offense.

What would you do if you found a piece of paper with the email address and password of someone whom the media claimed was a suspect of child abuse? You would perhaps consider handing over the paper to the police, hoping they would be able to log in and read through emails that could help provide evidence. Whether the police is allowed to log in is legally still a "grey area" as is breaking into a server or computer whose physical location is unknown to them in advance. The pressure to gather evidence and the ambiguity which still exists concerning legislation regularly presents dilemmas to detectives as they go about their work.

Consequences

The powers under the Special Police Powers Act (BOB legislation) are often not adequate to allow digital and internet detectives to take the actions mentioned above. According to the principle of legality, criminal prosecution may only take place when authorized by law. Therefore the police cannot "make up" any authorizations. As a result detectives, sometimes without consent of the public prosecution, take their own decisions on actions in a digital investigation. In the court room, this may result in evidence being excluded. If a detective has logged in to a server located abroad, this can even have personal implications for the detective in question, and she/he may be subject to prosecution for computer intrusion in the particular country.

False key

Why is there debate on whether details found by police can be used to log in? That, is due to a number of definitions in legislation and in case law. A good example is a search. If the police want to search a home, this will require a search warrant from the delegated judge. If the police have the key to the home, they will usually use the key to enter the home.

If the police do not have a warrant from the judge giving permission to enter the house, the police could be guilty of breaking in using a false key. Whether the key is physically genuine or copied is irrelevant in this context. The falseness lies not in the key itself, but in the unlawful use of it. The key itself is real, but its use is "false".

A computer is not a location

A search warrant does not suffice to search a computer. After all, the Code of Criminal Procedure only talks about searching a location or a means of transport, and a computer does not fall under either of these categories.

Since the law does not recognize any clear jurisdiction for the police to for instance log into to a suspect's Facebook account or a server, the police may be using a false key once they log in nonetheless. In doing so, they would be making unlawful use of a "key" they may have found, in this case the login details, which is prohibited[1]. None of the BOB powers mention a jurisdiction to log in/break in to servers whose physical location is unknown.

Anything is allowed, with permission

A common saying at the police is: "Anything is allowed, with permission". This is because the law mainly permits acts which the police may exercise against the will of a civilian or business. If a person, however, consciously gives permission to the police to perform an act, there can usually be no objection to this. This is not always the case for computers. In certain cases, for example abductions or murder cases, it may be important to read the (personal) messages of a victim on his or her social media account. These accounts may contain clues about the victim's last location and the last person he or she had contact with. Sometimes the immediate family members have the password to the victim's account and want to provide this to the police. Unfortunately, the general terms and conditions of Facebook, for instance, state that account details are not transferable. Not even after the account owner's death. The family does therefore not have the right to give police permission to log in to the account. It should be noted here that this is a civil-law problem and would most likely not have any drastic consequences in a criminal case against a suspect (provided it is the victim's account being accessed and not the suspect's).

Temporary solutions

Nonetheless the police do have some possibilities of obtaining the required information without an immediate need for amending the law. In the event of email accounts and websites, it is usually possible to use a BOB warrant[2] to demand the user's identifying details. This could include IP addresses, name, telephone number, and date of birth, for instance. If the content of the emails is important, a mutual legal assistance request (MLA request) is often required. This could take months, however. If email contents from US providers such as Hotmail and Gmail are involved, this also usually requires what is referred to as "probable cause". This means that the police must first be able to demonstrate more or less what they expect to find. A request for specific emails must be submitted. Police cannot request the entire inbox.

A request for identifying details often takes between a few days to a few weeks and can take place without an MLA request, based on an agreement between the Netherlands and the US. For the rest, in the event of a life-threatening situation, most US companies cooperate more quickly, provided the police can adequately demonstrate the imminent danger to a person's life or safety.

---

[1]Section 90 of the Code of Criminal Procedure, 311 of the Code of Criminal Procedure and LJN-AI1588.

[2]The law does have another section, specifically one that provides for a search in order to record data (section 125i and section 125j of the Code of Criminal Procedure). This must however involve a computer that is turned on in the home/location of a search. The police must therefore physically be in the same location as the computer in question, from which access is provided to another computer on the same network.

Dark web

It is only possible for warrants to be issued and MLA requests to be made if the police know the identity of the administrator/service provider of the required information. If the dark web is used (anonymous networks such as TOR, Freenet, and I2P), that is usually not the case. On the dark web, users regularly make use of anonymous providers and so the police cannot demand any data. Using login details that have been found or breaking into the server would, in that case, be the only possibility of recovering the required information.

Legislative proposal on Computer Crime III

Some of the now-known "hack-back act" attempts to solve the problems outlined above. In the event of extremely serious crimes, this law allows the police to investigate servers whose physical location is unknown and investigate the computers of private individuals, for instance. This is odd, since Dutch law cannot confer any power to conduct criminal investigation in the territory of another country. As is the case if a server hacked by police emerges to be located abroad.

The decryption order, an order imposed on a suspect to provide his password on penalty of a three-year prison sentence, has already been abolished. The question is how much of the controversial law will remain in practice.

The legislative proposal is controversial because people are worried that the police will be able to break into and look around on civilian computers without good reason. There are concerns about citizens' privacy. However the legislative proposal contains strict safeguards including the requirement that permission must be given by a delegated judge and that an extremely serious crime must be involved, one which incurs a prison sentence of eight years or more (terrorism or human trafficking, for instance).

History teaches that amending the law is usually a lengthy process and that lawmakers are virtually always playing catch-up to the facts. For the time being police will have to work with the powers they do have to conduct investigation into criminal offenses in the digital world, such as warrants, orders, and MLA requests.

Conclusion

The legal dilemmas faced by many detectives during investigations are often the inability to log into accounts using details that have been found - or provided with permission - and the inability to search servers remotely. There is usually a great deal of pressure to log in nonetheless, in order to solve an important case or save someone's life. The possible consequences of gathering evidence without the authority to do so are not negligible, however. For example evidence can be thrown out or a detective may be criminally prosecuted for computer intrusion in another country. Digital and internet detectives currently have limited legal possibilities for collecting evidence digitally and tracking down suspects. The new legislative proposal provides more possibilities, but is still controversial.

About the authors

Fleur Tamsma, MSc, is a consultant at Capgemini. As a criminologist, she specializes in intelligence and cybersecurity and has experience with this in the public sector. Jule Hintzbergen is a consultant and cybersecurity expert at Capgemini.

For more information, you can contact the authors at:
fleur.tamsma@capgemini.com and
jule.hintzbergen@capgemini.com

Quantum computers crack encryption

Should you already be taking measures to protect your data?

The concept of quantum computers - computers that offer many new possibilities - has been around since 1981. Initially little credibility was given to the possibility of creating a quantum computer. The situation now is entirely different and a lot of money is being invested worldwide in the development of stable quantum computers.

Highlights

- In the Netherlands, research is being conducted at TU Delft into the creation of a stable quantum computer. A stable quantum computer could pose a danger to popular cryptography. The TU Eindhoven plays a leading role in the development of encryption that can withstand quantum computers.
- In the future an attacker will be using quantum computers to crack information from today.
- Consider taking measures now to start protecting your data!

Imagine: a new kind of computer that can solve difficult problems many times faster than the current generation of computers. Problems that would originally have taken millions of years to solve will suddenly be solved in minutes. This new kind of computer is on its way: quantum computers. This makes it possible to perform advanced simulations, for instance, and in doing so conduct fundamental investigation into matter. However this technology brings not only advantages with it. Quantum computers make it possible to crack certain commonly used cryptographic algorithms much more quickly. It could be years before quantum computers are operational. Still, it would be wise to start considering measures already. In the future, quantum computers will be cracking the communication of today.

Quantum computers

Quantum computers are computers that make calculations in a fundamentally different manner than today's computers. They are therefore able to perform some calculations much faster. These computers currently only exist in experimental form. They are not yet suitable for accelerating calculations. A great deal of research is being conducted into the development of this new generation of computers. Research institutions in particular are working on this. Quantum computers are expected to have many valuable applications in the areas of biology and material science. The TU Delft expects to build a quantum computer between 2030 and 2040 which will be so immense that it will pose a danger to cryptography. It can be expected that it is not only research institutions, but also intelligence agencies which will be interested in building quantum computers.

Vulnerable cryptographic algorithms

Quantum computers will have a drastic impact on how we perform cryptography. All the current popular assymetric cryptographic algorithms are very vulnerable to be cracked by quantum computers. This includes algorithms like RSA, Diffie-Hellman, and ECDSA. These algorithms will be entirely ineffective as a counter measure against an attacker who has a working quantum computer. Asymmetric algorithms are also referred to as "public key" algorithms.

Asymmetric algorithms are often used to exchange keys. This takes place in protocols for secure connections (TLS, for securing the communication with websites) and virtual private networks (VPN, such as IPSec). Connections that use forward secrecy are also vulnerable. If an attacker cracks the key exchange, he can then see all the communication that has been encrypted using this key.

Other cryptographic algorithms are also vulnerable to attacks using quantum computers. Symmetric algorithms and hashing algorithms are both easier to attack using a quantum computer. Attacks using a quantum computer are less effective in this context, however. Doubling the key length used keeps attackers with a quantum computer away from your data that have been encrypted using a symmetric algorithm. Much less of a speed advantage can be achieved using a quantum computer in this context.

Cryptographic algorithms for encrypting data can be divided into two categories: symmetric and asymmetric algorithms. With a symmetric algorithm, both parties have the same key, which is suitable for both encrypting and decrypting data. With an asymmetric algorithm, each party has a key pair consisting of a “padlock” (the public key) and a secret key. Any third party can encrypt data using the padlock, but only the party which has the corresponding secret key can then decrypt the data. Most practical applications use both symmetric and asymmetric algorithms: this is called hybrid encryption.

The consequences of cracking keys using quantum computers

Someone with a working quantum computer can decrypt data that has been encrypted using vulnerable cryptographic algorithms. Data that is intercepted now can also be cracked in the future once a quantum computer becomes available.

At first it will be intelligence services and academic institutions that will have quantum computers. After all, they are currently the parties most active in developing a working quantum computer. In the long term, the capacities of quantum computers will also be within the reach of many business for example as a cloud application. It is conceivable that economies of scale will result in lower prices, which could make quantum computers affordable for individual consumers as well.

What should I do to keep my data secure?

It will be years before operational quantum computers are available. If data does not need to remain secure for that long a period, no additional measures are required. If you feel it is important to protect your data for a longer term it is necessary to start taking measures. After all, attackers may already be intercepting these data in encrypted form in order to crack them later. Perform a risk analysis to see whether your data require this kind of protection.

If you want to protect a link between two points against a (future) attacker using a quantum computer, use a symmetric algorithm like AES, with a key length of 256 bits. Exchange the key used manually, for example by having one or more persons with USB sticks (containing the key) travel from one point to the other.

Quantum Key Distribution (QKD, sometimes also referred to as quantum cryptography) is being sold as a solution for the problem of key exchange that can withstand attackers with a quantum computer. However the security features of QKD systems are still understood only to a limited extent and QKD is still hardly standardized. The use of QKD also requires expensive hardware. Therefore it is very doubtful whether there are cases in which QKD can make a valuable contribution.

Future solutions

In the longer term, we will all be switching to algorithms which are not vulnerable to attacks using quantum computers. For symmetric algorithms, this means lengthening the keys. For asymmetric algorithms, it is a bit more complicated. There are asymmetric algorithms which are not susceptible to quantum computers. These are still not as efficient as the algorithms popular now. They have also been standardized only to a very limited extent. Commonly used encryption software, therefore does not support them yet.

The development of this kind of post-quantum cryptography is still primarily an academic matter. The EU and the Netherlands play an important role in this. The EU program Horizon 2020, for example, funds a research consortium of eleven universities working on the development of quantum-resistant algorithms. This consortium is headed by TU e-professor Tanja Lange.

About the authors

Pieter Rogaar, MSc, is cybersecurity advisor at the Dutch National Cyber Security Center. He is specialized in cryptography and enjoys immersing himself in issues concerning ICT law. Ton Slewe, MBA, is an advisor at Capgemini. He focuses on cybersecurity issues at public and private organizations.

References

Information sheet from NBV about quantum computers:
https://www.aivd.nl/publicaties/publicaties/2014/11/20/informatieblad-overquantumcomputers
Position of CESG (division of GCHQ) on QKD:
https://www.cesg.gov.uk/white-papers/quantum-key-distribution
Commercial National Security Algorithm Suite and Quantum Computing FAQ, Information Assurance Directorate, National Security Agency/Central Security Service, January 2016.
https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf
A gentle introduction to post-quantum cryptography"(Dan Bernstein and Tanja Lange, CCC):
https://events.ccc.de/congress/2015/Fahrplan/events/7210.html
Website of the PQCRYPTO EU project:
http://pqcrypto.eu.org/

For more information, you can contact the authors at:
pieter.rogaar@ncsc.nl or ton.slewe@capgemini.com

How the Internet of Things can increase security in the transportation sector

Does the development of the Internet of Things present opportunities for the railroad to be more efficient for the operator and more efficient and easier for passengers?

The Internet of Things (IoT) has enormous potential for the transportation sector. Not only can planning and maintenance processes be set up much more efficiently, transportation security can be increased significantly as compared to security systems in which no linking of information takes place.

Highlights

- The preconditions for making the Internet of Things (IoT) a success are increasingly present.
- IoT not only has the potential for making more effective transportation and maintenance possible, it can also increase safety.
- The increase in safety applies for the infrastructure and the means of transportation themselves, but also for the passenger and driver as user.
- Applications are sensitive to malicious (and other) disruptions; risk management must therefore be carefully considered in advance.

The IoT consists of sensors, linked to objects, which send information and notifications about themselves. The IoT is not new and although the possibilities for application are being further investigated, it is recognized that it has the potential to drastically change the way in which we live and work. In order to get an overview of the potential impact, it is a good idea to specify precisely what the IoT entails. Although different definitions are used, we can identify a number of elements which at the very least part of it:

- There is a network of physical objects.
- These objects are equipped with sensors that collect, process, and send information.
- These objects are equipped with a direct or indirect internet connection.
- The communication between the objects takes place independently; in other words, the objects are “smart”.
- Sometimes the use of cloud computing is also added to this, whereby the data collection or even the data analysis takes place in the cloud, after which it becomes available to the user.

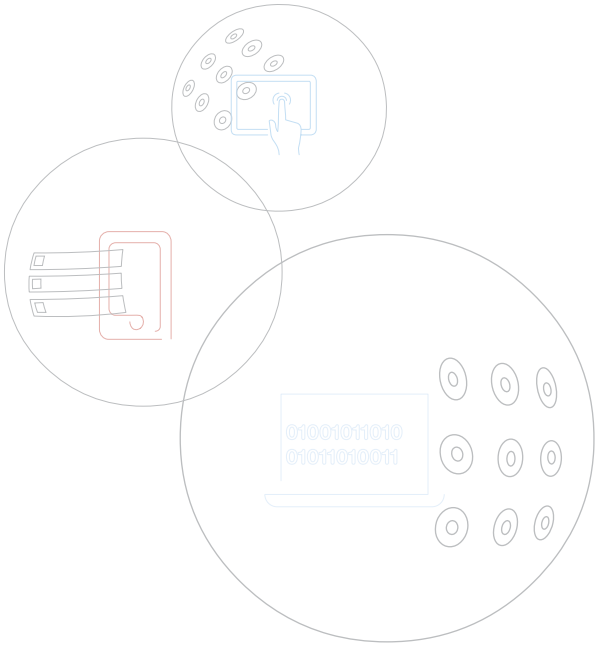
We are still only at the beginning of a major development which will continue in the years to come. The number of sensors linked to the internet or other networks - currently already in use in approximately one billion devices - will grow exponentially in the years to come. Estimates of the growth show that this will take place in the coming five years. Business Insider predicts that the market volume for IoT objects in 2019 will be more than double than the market for smartphones, tablets, PCs, wearables, and linked cars together and will comprise roughly about some 25 billion linked objects[1].

Developments that contribute to the high expectations for IoT are the rapidly growing bandwidth for data exchange, the market penetration of smartphones (as a means of operating the IoT),

as also the increase in other devices in which sensors have been built in. New technologies are becoming increasingly inexpensive and are therefore boosting applicability. An example of this is LoRa, a “low range” and “low power” network, specifically suitable for end-to-end encrypted communication between devices which require very little network capacity. This makes the network ideally suited for sensors with a limited flow of information. A LoRa transmitter has a reach of ten kilometers, a battery life of five years, and is inexpensive. A comprehensive network can be set up everywhere. It is no surprise that telecom operators are stepping up the rollout of LoRa networks[2].

In addition to the use of the network, software and hardware which facilitate communication between objects are increasingly becoming easily available. Arduino and Raspberry Pi, for instance, provide small computers the size of a credit card which can be linked to objects and easily programme themselves.

So what is standing in the way of widespread unfurling then? In the 2015 edition of Gartner’s hype cycle[3]. IoT is currently in the “peak of inflated expectations”; companies are achieving success with early applications of the phenomenon, but there are also a great many initiatives and technology providers that are not succeeding.

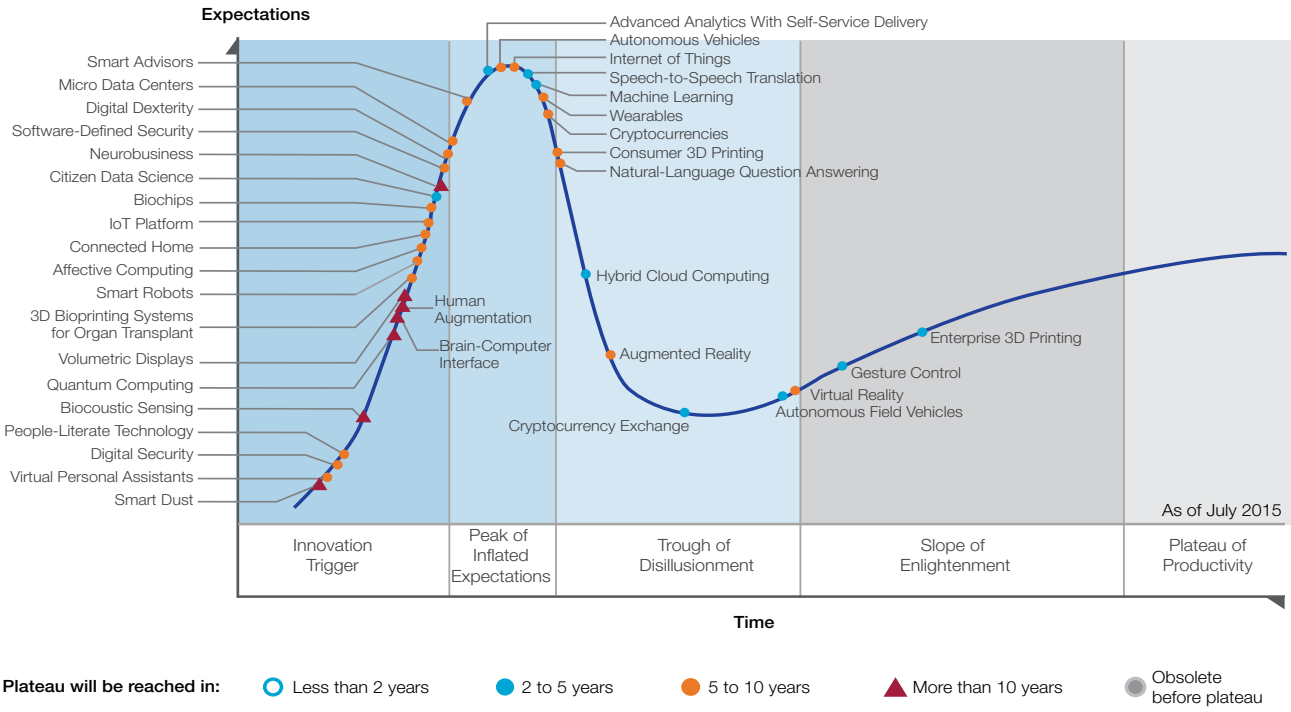


[1]http://uk.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10?r=US&IR=T

[2]https://www.kpn.com/ss/Satellite/obnWtwUWXNWZ5PBGmrg7Cn1efX49TLV50t-mOotPpXvR_aCibqpBz4G_pxjG_cNs0/MungoBlobs/attachment/ LoRa_brochure_NL_WEB-2.pdf

[3]http://www.gartner.com/newsroom/id/3114217

Figure 1: Hype Cycle 2015 by Gartner



Concerns about security also play a role. In 2015 and 2016, objects ranging from Barbie dolls to Jeeps were proven to be susceptible to hacking. Attacks focus generally on the weakest link in the chain. This means that security between the various objects needs to be looked at closely, especially if there are multiple suppliers. Problems that can arise here include, for example, the fact that updates are difficult to carry out and it is not always clear who is responsible for carrying them out. The types of companies that are developing IoT applications are also often not very interested or specialized in the security of the software used. They are more specialized in the production of devices.

Only when good solutions for these kinds of problems are common property and the business case for investments is irrevocably positive, is it likely that use will take off[4]. For applications of IoT, reference is usually made to examples of household appliances or cars. There are also examples, however, that provide a peek at the future of IoT on a larger scale as well. In so-called smart cities, buildings and infrastructure will, in a few years' time, be providing information on their state of repair; and roads will report the current traffic conditions and parking availability. At the same time, monitoring is taking place of noise in nightlife areas, the quantity of trash in containers, the air quality, and the volume of pedestrians in order to be able to quickly take action and enable tailor-made services[5].

A good example of the possibilities for using IoT in the railroad is the telecom department of Network Rail, the UK rail infrastructure management company. Since 2014, Network Rail has been working on increasing its internal service offerings, and at a later stage its external service provision[6]. As the responsible party for the lights, signals, train radio, switches, travel information, etcetera, they made a start by creating internet connections to the sensors already in use. For example, sensors that measure air and rail temperature or metal tension. The rationale is that combining information improves the maintenance and planning process, work and rail safety, information provision to passengers and finally cost management for all of this.

While many man-hours are currently lost on physically inspecting the many kilometers of rail, sensors that monitor the environment or the objects themselves, in combination with visual information from cameras at fixed points and on trains, can provide enough information to facilitate remote checks and monitoring. This allows the status of and defects in the rails, overhead lines, switches, and other matters to be kept track of centrally.

The linking of sensors on the train itself provides the same possibility for planning the maintenance process more efficiently. The train itself can indicate what needs to take place at what moment in terms of cleaning or maintenance. Trains are already equipped with sensors but this information is often only available locally or limited to parties that could benefit from it. Information to passengers about a train's precise location or what areas of the train are full or nearly full can help passengers better plan their journey.

---

[4]https://www.capgemini.com/resource-file-access/resource/pdf/the-internet-of-things.pdf .

[5]http://www.journals.elsevier.com/future-generation-computer-systems/call-for-papers/special-issue-on-smart-city-and-internet-of-things/.

[6]http://www.computerweekly.com/feature/How-the-Internet-of-Things-could-transform-Britains-railways.

[7]Capgemini Consulting (2014) Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT.

The most important potential gain lies in having trains run more safely. In the past decades, a great many initiatives were developed which made enormous improvements to safety on the rails. In the coming years, traditional safety systems will slowly be replaced with more digital variants and the use of sensors will increase even further. While trains were initially only equipped with what was referred to as a "dead man's switch", it was not long before signals started being sent to the train via the tracks. The first generation of automatic train protection (known as ATP) sends electrical signals via the tracks, passing on speed limits to the driver. If the driver does not obey the speed limits, the driver receives a signal. If the brake is not applied, the system automatically intervenes. Improvements have been implemented in the second generation of ATP via warning systems like ORBIT, which works based on GPS signals. The greatest opportunities for IoT, however, lie in linking the data that is already available, such as those from the train and infrastructure. In the future, further development can take place by joining the introduction of the European Rail Traffic Management System (ERTMS).

Trials are currently being conducted with ERTMS, which is aimed to partially replace ATP. ERTMS establishes a European safety standard. In the long-term, the traditional ways of signaling, pulsing, and lights will be replaced with a system in which the cabin automatically receives the data. The advantage is that the tracks can be divided up into much smaller segments and that trains can consequently drive more efficiently and closer to each other.

Ultimately, trains will communicate with each other. This communication uses GSM-Rail, which is transmitted on a unique frequency. Although the rollout of ERTMS has been delayed and is yet to start, it is certain that the system will be established and will serve as the safety standard in years to come. The system provides excellent opportunities to link the information from sensors in order to increase safety maximally. For example, traffic control which can adjust a train's speed based on information on the status of the infrastructure.

Aside from the link with ERTMS, rail safety can also be improved via the human side, namely via the driver of the means of transportation. One of the key indicators for rail safety is Signal Passed at Danger (SPAD), whereby a red signal is passed. Until now, analyses on SPADs have often taken place in relation to incidents in which a signal was passed or this passage was narrowly avoided. The normal situation has been little explored in this context, however. This makes it difficult to compare circumstances during incidents with normal day-to-day use of the rail system. Sensors in the cabin can enable far more data on the air quality, temperature, light conditions, degree of tiredness, concentration, and distraction to be linked with each other. This data could also be automatically responded to, so that the most optimal climate for a particular person is always maintained in the cabin. Data on distraction and concentration can also be analyzed and combined with data on braking, location and speed.

Conclusion

The development of the IoT presents enormous opportunities for making rail transport more efficient for the operator and more efficient and easier for passengers. Research by Capgemini Consulting indicates that some of the biggest hesitations among producers when it comes to using the IoT are rooted in concerns about how the devices and communication channels are secured[7]. The risk factor for using IoT in relation to the railroads is enormous, since human lives could be at stake. Solutions will therefore have to be completely solid. It is also clear, however, that having a more accurate picture of the entire rail network can improve safety substantially. The choices that make safety and efficiency priorities are very important.

About the authors

Roy Oudeman, MSc, and Melle van den Berg, MSc, are both managing consultants at Capgemini Consulting. Roy helps organizations design and implement security and safety management. Melle is a specialist in cybersecurity and crisis management. Melle worked on the Capgemini Consulting study "Securing the Internet of Things".

Merlijn Mikkers is Safety advisor at the Dutch National Railways and Phd candidate at the section Safety and Security Science of TU Delft.

For more information, you can contact the authors at:
roy.oudeman@capgemini.com, melle.vanden.berg@capgemini.com and @mellevdberg



Biometrics: A future without passwords?

To what extent can the secure use and storage of biometric data for authentication be guaranteed?

While there is often opposition to the use of biometrics in government applications, it is being used increasingly and more widely in the consumer market, and consumers appear to be embracing it.

Highlights

- End of the password era?
- Biometrics has become an intrinsic part of authentication.
- Guaranteeing the secure storage of biometric data is essential for success.
- Clear and transparent policy on biometric applications is lacking.

Although biometrics are already put to much use by government agencies, the use of these biometric methods met with resistance. Users do not like providing biometric data because they feel this violates their privacy. People also wonder how securely these biometric data are stored. Experts agree that because of difficult to manage organizational and human factors, the large-scale use of biometrics can only be made adequately secure with a great deal of extra effort. In assessing the security of a biometric application, it always concerns the entire application, so including technology, organization, procedures, and the degree to which people are involved or in fact have an interest in errors or abuse. Errors or abuse are generally not in anyone's interest when the solution involving biometrics is mainly considered for its ease of use.

The use of biometrics in the consumer market is on the rise. There you see more and more applications that use biometrics as a means of authentication. For instance, MasterCard users already have the option of making credit card payments using a selfie or fingerprint as authentication.

Customers can make purchases at online shops using a selfie and renew a phone contract using voice recognition. The most common example of biometric authentication is the fingerprint used as authentication for a smartphone.

Although there is strong growth in biometric applications, it is only a question of time before various biometric applications are abused, in one way or another. In these kinds of cases, the government must ensure policy and legislation aimed at preventing the abuse of biometric data and identities based thereon.

Biometrics

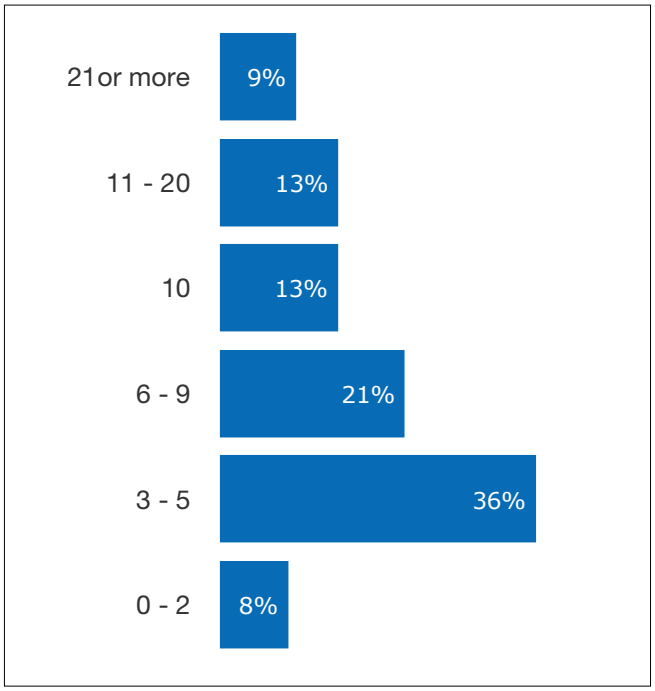
Biometrics refers to the recognition of persons by means of a physical characteristic and using information technology. If a customs official uses the naked eye to compare the individual in front of him to a passport photo, this is not biometrics. When this takes place in an automated manner, we do speak of biometrics.

When a person is recognized based on biometric data, a physical characteristic measured earlier is compared to the result of a new measurement. Biometrics is much more than fingerprints alone. It can involve voice characteristics, patterns of the iris in the eye, the rhythm of a person's typing, body odor, DNA, or the movements a person makes when writing. All these forms of biometrics can be used for biometric person recognition and can be applied as a means of authentication.

The question is: what form is the most reliable and is at the same time user-friendly enough and involves relatively low cost to become accessible for the larger public? Vein analysis under the fingerprint is extremely reliable, but very complex for ascertaining within a short timeframe whether there is a so-called match. For the time being, fingerprints are the most widely used form of biometrics. Not only can a comparison be made within a short timeframe, it is also reliable. Nonetheless, false positives can also sometimes arise.

The scope of application for biometric methods is expanding rapidly. The importance of person recognition has increased because we find ourselves in an anonymous information society with a growing worldwide mobility.

Figure 1: How many different types of password are you currently using to log in to websites, email accounts and other accounts?



Biometric methods are also a solution for the difficulty of remembering numerous pin codes and passwords. Research by TNS NIPO indicates that most Dutch people currently use between three and nine passwords; one third of respondents even report that they use more than ten passwords. In this situation, the use of biometrics sounds like a much more efficient means of authentication.

Government services and biometrics

The use of biometrics for private applications is on the rise, but government agencies have long been making use of biometric data. The Dutch biometric passport is one of the most striking examples of this. This passport contains a chip on which the holder's data is stored, supplemented with invisible data. At border checks, the biometric data of the traveler can be compared to the biometric data on the chip in the passport.

The initiative for the biometric passport existed even prior to 2001, but the development was stepped up due to the attacks of 9/11, partly because the United States threatened to exclude European passports without biometric features from the Visa Waiver Program. The key aim of the biometric passport is to prevent so-called "look-alike fraud", i.e. a person using another individual's passport. In practice, it had emerged that people are not very good at comparing a passport photo to a person in the flesh. Trained professionals score just slightly higher than untrained people when it comes to identifying frauds. Facial scans and fingerprints analyzed by a system should now ensure that this type of fraud can no longer take place.

Ease of use versus security

There does emerge to be considerable public support for biometric applications. But the user does not have the sense that every biometric application is equally reliable and secure. People are most confident that the Tax and Customs Authority - DigiD, hospitals, and banking institutions handle data securely. Take ABN AMRO, for instance, where users can take care of their banking via a fingerprint, which has given rise to little protest. According to TNS NIPO's survey, people have the least trust in developers/providers of apps for smartphones. Six in ten have no trust in these parties when it comes to securing data. It also emerged from this survey that web shops and Google are not trusted when it comes to handling personal data carefully.

Nonetheless, it emerged from the same survey that for almost seven out of ten Dutch people, the main concern when installing an application is whether the app is free; only one third takes into consideration privacy protection.

There are many new possibilities with smartphones today, for instance, by improving the camera which can also be used to make a decent iris scan. This could enable you to pay at web shops using a selfie.

The degree to which biometrics is becoming accepted is growing, but like any form of authentication, biometrics has both advantages and disadvantages.

The flipside of ease of use

Before the launch of the iPhone 5s, biometrics was never really applied on a large scale outside of governments and secret services. This is mainly because the benefits do not outweigh the still considerable costs of purchasing readers and middleware and the challenges in relation to privacy. In 2013, however, soon after the launch of the iPhone 5s, a video appeared on the internet in which hackers showed how, using a photo of someone's fingerprint, they could make a forged fingerprint to unlock the phone.

Biometric data can fall into the wrong hands. This has major consequences since, unlike a password, biometric characteristics cannot be changed. So once a piece of biometric data has been abused, this piece of data is rendered insecure for all applications that use the particular data. The risks in relation to the storage of biometric data are also growing. Privacy is in jeopardy because databases are increasingly linked to each other, for instance in the fight against international terrorism and organized crime. The data is stored at more and more locations, therefore significantly increasing the risk of hacking. Good encryption and hashing (creation of a hash code from which the original data can no longer be derived without a key) of biometric data is a requirement here.

Conclusion

With more and more forms of biometrics are being used for authentication, the risk of abuse of data is increasing. Once a piece of biometric data has been abused, it cannot easily be replaced. You cannot replace a fingerprint, for instance. People want ease of use, but also want the guarantee that it is secure. It is essential to find a balance between the two. A choice for more ease of use does not automatically mean that security can be optimally guaranteed. Authentication based on biometrics is now mainly assessed from the perspective of ease of use: in order to replace the commonly used (but often forgotten) passwords and pin codes. While in other areas "security by design" is receiving greater attention, the tendency in biometrics seems to be the opposite, in order to keep the use of biometrics low threshold and optimize the scope of application.

In order to ensure that biometrics as a means of authentication is a success, two matters are of essential importance. Firstly, secure storage of biometric data must be guaranteed by exclusively storing these locally, for instance. Secondly, the government must devote more attention to new applications using biometrics. As indicated earlier in this article, abuse of these data is only a matter of time. If the identity (biometrics) of a person is stolen, this is not just a major problem for the person him or herself. This can also pose problems for the organization where this person is employed, which has set up authentication on the basis of a biometric feature. In that case, it is not only the digital security of individuals which is at stake, but also that of organizations and the business sector. The faster the developments move, the faster the government must be able to respond to these. Otherwise, a person will be able to pose as someone else unpunished, with all the consequences that ensue from this.

About the authors

Sjoerd van Veen, MSc, and Gijs Daalmijer, MSc, are both consultants and public administration experts and, as such, are active in the domain of public order and security.

For more information, you can contact the authors at:
sjoerd.van.veen@capgemini.com and gijs.daalmijer@capgemini.com

Influencing people is child's play: Arm yourself against social engineering!

How can you protect yourself and your organization against influence from cyber criminals?

Social engineering is an attack technique in which human characteristics are abused in order to obtain confidential information or tempt someone to perform a particular action. This article explains the psychology behind social engineering, outlines what technological means cyber criminals are using in 2016, and shows how people can arm themselves and their organizations against these.

Highlights

- Social engineering is the manipulation of human behavior by using principles of influence.
- People exhibit preprogrammed behavior which cyber criminals abuse.
- Social engineering is being put to increasingly wide use via digital channels.
- Learning from experience can make individuals and organizations more aware and less vulnerable.

In information security, humans are often described as the weakest link. Despite all the security measures such as firewalls, passwords, and even security personnel aimed at keeping intruders out, it is sometimes as easy as child's play to gain access to confidential information by using techniques of influencing human behavior.

Human behavior and the protection of confidential information are closely interlinked. Without realizing it, an inattentive individual can open the digital doors to hackers and give them access to confidential information, which can be used to commit identity fraud, for instance. People are constantly manipulated, influenced, and misled. Not only by advertisers, call-center employees, web shops, and car salesmen, but also by colleagues, friends, and indeed cyber criminals who want something from them. We increasingly see that cyber criminals prey on people's vulnerabilities and do so on a broad scale.

The psychology behind social engineering

A great deal of research has been - and is still being - conducted into human behavior. How can human behavior be explained? Why is it that people fall for phishing emails en masse and without hesitation we give social engineers access to our confidential information? A well-known behavioral researcher, Robert Cialdini argues that there are six universal principles of influence which determine human behavior. Social engineers use these principles of influence to manipulate their potential victim and provoke certain behavior. The six principles of influence are:

Reciprocity: The urge to have to compensate for what others have given us. Having the sense of owing someone else something makes it easier than normal to honor a counter request.

Commitment and consistency: The urge to act in accordance with what we have done/said in the past. If we pronounce an opinion or make a decision, we have the tendency to act in accordance with similar past choices in future situations as well.

Social proof: Our view on correct or incorrect behavior depends on the behavior of others. If many people perform an action in the same way, we label this as correct.

Sympathy: Failing to honor an urgent request is unfriendly. If pressure is exerted by the description of a recognizable situation, this already makes it a bit more difficult to refuse a request.

Authority: From birth, we are taught that obedience to good authorities is the right thing to do. Because they have so much power, it often seems wise to obey these authorities. Who is suspicious of a fireman who comes to check the smoke detectors?

Scarcity: There are some things we start to value more as their availability decreases. If there is only one item in stock, we quickly have the tendency to think that we should take the opportunity before it is too late. At the chance of losing something, we have the tendency to put up strong resistance (greed).

In addition to the six principles, the time that someone is given to make a decision on the right action also plays an important role. During a social engineering attack, a victim must often respond within a short timeframe. For instance, phishing emails regularly threaten to block bank cards and accounts if the recipient does not respond within 24 hours by logging in to a bank login portal which looks legitimate but which has been forged by the hacker. The victim bases his or her decision on the limited information provided at the moment and if the above principles are applied successfully, the victim will trust in the content due to the time pressure. That trust is increased, for instance, because many phishing emails contain personal information relating to the potential victim, such as their full name, address, or bank account number.

In addition to the trust mentioned above and the tendency towards greed, it emerges that people are above all curious. People want to acquire what they do not yet have and, more importantly, avoid losing something that they do have. So if someone really wants something, he will briefly let go of his negative or suspicious feelings. For instance, the number of cases increases strongly when random users are phoned from "faraway" countries and the phone is hung up immediately after it is answered. Driven by curiosity, the victim returns the call and ends up phoning an expensive pay service (a kind of premium or 0900 number), resulting in a gigantic telephone bill.

Used increasingly widely

While social engineering was initially only used to gain entry to physical locations, over the course of time various technical aids have been developed that enable cyber criminals to carry out their attacks on a large scale and via digital channels:

- Phishing by email and telephone: According to the "Cyber Security Beeld Nederland 2015" (Cyber Security Picture of the Netherlands 2015. A report published annually by the NCSC), phishing turned out to be one of the most powerful and most commonly used attack methods by cyber criminals in 2015. Phishing is the collective term for digital activities aimed at persuading people to hand over their personal information (such as login details). The principles of influence used include: authority, scarcity, trust.
- USB drop: Cyber criminals are increasingly using USB sticks containing malicious software. These are, for example, dropped into a victim's bag during a train journey, left behind or handed out. When the finder plugs the USB stick into his or her computer to find out who it belongs to, it is already too late: the hacker is in. Vulnerabilities preyed on include: curiosity and greed.
- Rogue WiFi access point: The cloning of (mostly public) WiFi hotspots recognizable to and trusted by the user enables smartphones to easily contact this access to the internet, which is controlled by the hacker. The hacker can then monitor and manipulate the victim's internet behavior. Vulnerabilities preyed on: trust and consistency.
- Combination of attack techniques. It can be even more sophisticated as well: a phishing email is often announced by a caller, who asks a number of directed questions on topics in which someone has a professional or personal interest. After this conversation, the caller sends the individual an email containing a link for the person to follow, with all the consequences that ensue. Ransomware and malware are also increasingly added to phishing emails as attachments, which means it is no longer even necessary to get the recipient to click on a link: just opening the attachment is enough.

Don't become a victim: arm yourself!

This prompts the question of whether people can adequately protect themselves at all against cyber criminals who make use of techniques to influence people. While we tend to say that if they are determined enough, cyber criminals will always find a way, it is important to take a number of important measures to reduce the likelihood of damage by social engineering.

For the individual:

- Efforts by businesses and the government to make people aware of the threats are a preventative measure that helps prevent damage. Think of advertising campaigns for safe internet use (from the Safe Internet organization in the Netherlands, previously: DigiBewust) and the well-known commercial "Hang op, klik weg, bel uw bank!" ("Hang up, close the webpage, call your bank!").
- Use two-factor authentication or login verification for access to, among others, Gmail, Hotmail, and social media

accounts. Even if they have your password, cyber criminals will not be able to log in without the second factor (for example, SMS code, fingerprint, token, or TAN code) or your direct permission (login verification).

- Disable the “connect automatically” option when using public WiFi networks so that you do not connect to a rogue WiFi access point.

For organizations:

- Social engineering assessment: during a social engineering assessment, a trained social engineer will attempt to penetrate an organization and gain access to the “crown jewels”. This would be a good measurement of the vulnerability of the physical security, which also raises awareness.
- Phishing audit: the most powerful means of making an organization defensible against phishing attacks is “learning by experience”. Many organizations periodically conduct a phishing audit. A phishing audit is a method for measuring and immediately improving employees’ security consciousness, by performing a controlled phishing attack and gauging the response. When organizing and conducting a phishing audit, account must be taken of various legal, ethical, and technical aspects. In order to prevent incidents, it is therefore advisable that these kinds of activities be carried out by a cybersecurity expert.
- Advanced cyber exercise as the ultimate test: combination of phishing, hacking, USB drop, and rogue WiFi access. During the simulated attack, the employees in question are tested and trained for their resistance.
- Technical measures: email authentication using SPF, DKIM, and DMARC and alerting the wider public to the features of authentic emails so that they can be recognized. It is also advisable to use two-factor authentication where possible in order to minimize the risk of unauthorized access. This is very important if systems can be contacted via the internet.
- For the government: continue to invest in awareness campaigns which constantly use different ways to draw people‘s attention.

Conclusion

It is still as easy as child’s play to gain access to confidential information by using techniques to influence people. Cyber criminals are therefore using these kinds of techniques more frequently and the development of technology enables them to use social engineering on an increasingly larger scale. In order to avoid falling victim to social engineering, private individuals, and employees, the government and the business sector alike will have to take the right measures to protect their confidential information. Training and raising awareness are a good first step in this direction.

About the authors

Jan de Boer, MSIT, is a managing consultant at Capgemini. His field of expertise is integrated information security. He specializes in the psychological and human aspects of information security. Social Engineering is his passion. Guido Voorendt is a cybersecurity consultant at Capgemini. He is active in the domain of public order and security, and is specialized in social engineering, privacy and identity, and access management.

For more information, you can contact the authors at:
jan.de.boer@capgemini.com and guido.voorendt@capgemini.com
@gvoorendt

Communication after a data breach is crucial for maintaining trust

How, as an organization in the security domain, do you set up communication after a data breach?

The Mandatory Breach Notification has been in effect since January 1, 2016. This requires a carefully structured communication strategy towards victims in the event of a data breach.

Highlights

- The Mandatory Breach Notification has been in effect since January 1, 2016.
- Organizations in the security domain often process personal data of an extremely sensitive nature.
- A data breach could result in loss of confidence among the data subjects.

The Mandatory Breach Notification has been in effect in the Netherlands since January 1, 2016. This means that organizations that process personal data must, in certain cases, report a data breach to the Dutch Data Protection Authority (Dutch DPA) and to the data subjects (the persons to whom the data relate). A notification to the data subjects is only required if these individuals may experience detrimental effects. But how, as an organization, do you determine whether this is the case and what exactly do you report? Notifying data subjects must be done with a great deal of care, perhaps most by government agencies that have a relationship of trust with the citizen. Think of the police, for instance, who process a lot of personal data from citizens and for whom it is crucial to have the public's trust. In order to prevent citizens' trust in the government from becoming damaged, it is important to set up clear communication towards data subjects concerning a data breach.

The Mandatory Breach Notification

The Mandatory Breach Notification is an amendment to the Personal Data Protection Act (Wbp).

The Wbp captures the most important rules for handling personal data in the Netherlands. The aim of establishing a reporting requirement was to limit as much as possible the consequences a data breach could have for the data subjects and as such contribute to maintaining or repairing the relationship of trust between the organization and the data subjects. The reporting requirement means that organizations (both businesses and governments) must notify the Dutch Data Protection Authority (Dutch DPA) within 72 hours if a serious data breach occurs. If data subjects could encounter detrimental effects as a result of the leak, they too must be notified. In the first quarter this year, the Dutch DPA received 1,000 reports of a data breach[1]. For all these reports, the organizations involved also had to consider whether data subjects needed to be notified. It is unclear in how many cases this actually occurred.

A data breach in the security domain

Organizations in the security domain often work with large quantities of (sensitive) personal data. The police work with witness statements on a daily basis, for instance. If these witness statements are accessed by an unauthorized person, for example the perpetrator of the crime, or are lost, this could have detrimental consequences for the witnesses. In the latter case, they will probably have to submit their statement again. Other examples of organizations in the security domain that work with a lot of sensitive personal data are penal institutions (criminal and medical data), courts, law firms (files) and Safe Home (the organization that provides safe houses for domestic abuse victims).

Due to the sensitive nature of the data in the security domain a data breach could have serious consequences for the subjects. That is why it is important, particularly in the security domain, to protect personal data as securely as possible and take adequate action if a data breach nonetheless occurs.

[1]https://www.security.nl/posting/466908/AP+ontvangt+1000+meldingen+over+datalekken

Adequate action means, above all, that organizations are transparent towards the data subjects by notifying them carefully if necessary.

Data breaches are particularly complex in the security domain, however. There could be serious side effects of not informing the data subjects. If not informing the data subjects is in the interest of protecting these individuals, a decision can be made not to do so. This is the case, for instance, if data have been leaked concerning children who have reported abuse by a parent. Normally the parents would have to be informed, but that is not desirable in this case. In these kinds of situations, it can be decided not to notify data subjects for serious reasons.

What is a data breach?

A data breach means that in the course of a security incident, personal data has been lost or an unlawful processing of personal data may have occurred (processing is any action involving the personal data, such as reading, copying, amending, deletion, or destruction). A security incident has occurred if there is the possibility that the confidentiality, integrity, or availability of information or information-processing systems is or could be put in jeopardy. Data may no longer be available (as the result of fire or destruction), for instance, or the data may be lost in some other way, without a current back-up copy being available. Unlawful processing has occurred, for instance, if persons have obtained access to information to which they should not in fact have access.

However well the measures an organization takes to prevent a data breach may be, it is impossible to rule it out entirely. That is why organizations must set up a process (from identifying data breaches through to handling them) so that a (potential) data breach can be handled carefully and efficiently.

When must a data breach be reported to data subjects?

As mentioned earlier, the purpose of the requirement to report data breaches is to limit the negative consequences that a data breach could have for data subjects (unlawful publication, reputational damage, and (identity) fraud or discrimination, for instance). Informing data subjects enables them to be alert to the possible consequences of the data breach and to protect themselves against those consequences as much as possible.

A data breach must be reported to data subjects if the data breach is very likely to have detrimental consequences for their personal lives. But when is that the case? Two questions are important in making a careful consideration of this:

Do the technical protection measures provide adequate protection, based on current security standards?

This mainly concerns the degree to which the data are inaccessible or incomprehensible for persons who are not permitted access to the data. If, for example, data have been encrypted using cryptography (encryption or hashing) or if certain other technical protection measures have been taken (such as remote wiping or pseudonymization of data), it can be concluded that adequate protection measures have been taken. It is important, in that case, that the measures satisfy the latest standards in relation to technical protection.

Is the data breach very likely to have detrimental consequences for the personal lives of the data subjects?

This question cannot always be easily answered. The law states that there are detrimental consequences if the data subjects could experience material or immaterial damage. It is then up to the organization where the data breach occurred to assess whether this is the case. A consideration must be made for each case, based on the circumstances. A factor that is important, for instance, is the type of data that has been leaked. If sensitive personal data has been leaked, such as a person's race (which can be concluded from a passport photo, for instance), political preference, health, or criminal record, there are always detrimental consequences for the data subject and the data subjects must always be notified.

Take the time now to think about the communication strategy

It is recommended that every organization prepares a communication strategy; and this can and should be thought about now. A communication strategy consists of three components: how will we communicate, what will we communicate, and who will do the communicating? The law only stipulates substantive requirements for the communication towards data subjects. How the communication should be set up, who is responsible for communicating, and what channels are used is up to the organization itself.

How does the communication take place?

First of all, there must be insight into what channels and means of communication are available for reaching the data subjects. The different target groups whose personal data are processed by the organization must be taken into account here. It is conceivable, for instance, that older people can better be reached via different channels than young people. Some older people may not have an email address and must be informed by letter or telephone call in that case. It is also advisable that two preparations be made in any event. Firstly, an overview should be drawn up of where personal data are stored: in systems, paper dossiers, or on external data carriers. This makes it possible to immediately figure out what personal data may have been lost if a data breach occurs. Secondly, it is advisable to prepare a data breach classification. This can be done based on who must be notified, for instance: only the Dutch DPA, the Dutch DPA and the data subjects, or no notification whatsoever. A team can be linked to every level, which springs into action in the event of a data breach. Taking these preventative actions means that if a data breach occurs, the communication strategy only needs to be adapted to the specific situation of that moment.

What to communicate?

The law stipulates three requirements for the content of the communication:

1. The nature of the breach: what kind of data breach has occurred, what happened? It is advisable in this context to at least inform the data subject whether it is certain that his or her data has been leaked. The risk estimate that someone could abuse the leaked data, or the risk that this might actually have happened, can also be reported.
2. The agencies from which the data subject can obtain information about the breach: the contact point to which data subjects can turn to with questions (email, telephone etc.).
3. Measures that you advise the data subject to take in order to limit the negative consequences of the breach. It is a good idea here to also explain what measures the organization itself has taken or intends to take.

Who will do the communicating?

In principle, the Data Protection Officer (DPO) is responsible for proper handling of a data breach, including the report to the Dutch Data Protection Authority and possibly to the data subjects. The DPO will not always perform the communication towards the data subjects, however; this depends on the circumstances and the type of data breach. If sensitive data has been leaked, it may be decided, for instance, to have the party that has had previous contact with the data subjects perform the communication now (for example, a police officer at the police department or a doctor at the hospital), while in the event of less sensitive data, a more general communication (by letter, for instance) may suffice.

Take action now!

If a data breach occurs, which can happen, action must be taken efficiently and effectively so as to limit (reputational) damage as much as possible and maintain or repair the relationship of trust. That is why it is important to be prepared in advance with a careful communication strategy (how, what, and who?) for the affected data subjects. This is especially the case for organizations in the security domain, because of the extremely sensitive nature of the personal data they process.

About the authors

Daphne Gerritsen, MA; Martine Middelveld, MSc; and Christian le Clercq, LLM MSc, are security and privacy consultants at Capgemini Consulting. They focus on privacy and security issues at public and private organizations in the security domain.

For more information, you can contact the authors at:
auteurs via: daphne.gerritsen@capgemini.com, martine.middelveld@capgemini.com and christian.le.clercq@capgemini.com



Digital security starts at school

How do school board members, teachers, and school pupils become more cyber aware?

Cyber threats and vulnerabilities are on the rise in education. Adequate awareness about the risks and the impact will make the school environment safer.

Highlights

- The school and education sector are becoming increasingly digitized, which in turn prompts the rise of threats and vulnerabilities.
- Owing to the rapid pace of developments, school board members and teachers often have too little knowledge about cybersecurity.
- School pupils are frequently early adopters of digital developments and need guidance on how to use digital resources wisely and safely.
- Raising awareness about cybersecurity in the school environment (among school board members, teachers, and pupils) plays a major role in ensuring a safe school environment.
- As a consequence of the strong mutual dependency, cooperation between the school and chain parties is necessary in order to be able to stand up to the cyber threats.

The education sector is becoming digitized. This presents new possibilities when it comes to simplifying administrative and financial processes, for instance, and offering pupils tailored educational opportunities. The flipside of digitization in the education sector is that the risks of digital threats and vulnerabilities of the school can increase, resulting in the possible victimization of the school, the employees, and the pupils. This problem will continue to grow as long as the school environment (school board members, teachers, parents) does not invest in cybersecurity awareness and consequently cannot provide insights to the pupils.

Digitization in education and at school

Society digitizes at a rapid pace. The complexity and the possibilities are growing[1]. Education[2] is also becoming increasingly digitized. Digitization has a double impact in this context.

Firstly, the school itself is going digital. The administrative and financial chain of the school and teachers' education are increasingly taking place digitally. The registration and deregistration of pupils in the MBO (senior secondary vocational education) sector takes place digitally, for instance. Data already on file at DUO are automatically generated and data from a previous school can be easily transferred. This makes registration and deregistration simpler, smoother, and less susceptible to errors[3]. The registration of grades and communication on these with pupils and parents largely takes place digitally as well.

Secondly, education is becoming digital as a result of adopting digital teaching methods and new knowledge on digital societal developments. Digital educational tools with new teaching methods are being developed by publishers and new players in the market in order to better tie in with pupils' learning needs. This contributes to faster and better development on the part of the pupil. Pupils receive the education they need instead of the education that is offered as standard. Secondary education and vocational education is also considering to what extent they want to make use of digital educational tools[4]. Not only educational tools, but tests like the standardized CITO test are also going digital[5]. These changes require different (digital) skills from the teacher.

It is not only the school and education sector that are becoming digital. Pupils themselves are doing more things digitally as well. For school pupils between the ages of 10 and 18, a large part of their lives is determined by media use and they have access to digital resources and the internet from a far younger age. Young people are often early adopters and are growing up taking for granted the fact that they can be online at all times, no matter where they are[6].

Threats and vulnerabilities

The flipside of the digital school and digital educational tools is that schools are increasingly dependent on the continuity and security of their systems. Schools also work with extremely privacy-sensitive information (such as test results). Threats and vulnerabilities increase with the growing use of these digital (educational) tools. These vulnerabilities can also be maliciously abused. The first cases of ransomware and cryptoware[7] have already been encountered in the education sector. There was a story recently in the news in which a US school paid 8,500 dollars to internet criminals who managed to encrypt several school servers using ransomware[8]. Threats can, however, also come from pupils. The current generation of young people is growing up with the fact that all information can be found on the internet – including knowledge about carrying out a cyber attack. What if a pupil does not feel like taking the exam? A DDos attack is easy for this generation to carry out or "order" online. Did a pupil get poor grades this term? Committing fraud by breaking into the school's system may not be easy, but it is possible. The damage resulting from these kinds of actions runs into the millions each year[9].

Today's education for creating digital awareness is inadequate

Threats and vulnerabilities in relation to both the environment (systems and digital educational tools) and the users (teachers and pupils) come together in the ecosystem of the school. From the perspective of their own subjective experience, pupils are immersed in the development of the digital world. More and more jobs require technological knowledge and skills[10]. In addition to arithmetic and language, the skills for the 21st century include ICT literacy and creativity, for instance[11]. In order to prepare them for day-to-day life and the labor market, they must be guided through this ongoing digital transformation.

At the primary school, children learn to deal with ICT and they learn about risks posed by the internet via initiatives like mediawijzer (media guide), the codeweek.nl, and the national curriculum debate[12]. As soon as they reach secondary school and vocational education, they have a backpack of knowledge. In secondary education, classes that can make them media savvy are offered (programming, cyber bullying, social media), but the content and implementation of these classes is determined by the schools themselves. There are still no clear educational lines: there is little theory in education that can help one become media savvy, the existing teaching material is often difficult to find, and teachers are not properly trained and more importantly have enough work teaching their own subject[13].

School board members are not adequately cyber aware

Research shows that the education sector is vulnerable when it comes to cyber crime, and that school board members do not yet have adequate cyber expertise. School board members underestimate the potential consequences of incidents[14]. Teachers also indicate that they do not have sufficient knowledge and skills to use ICT in education and are therefore unable to transmit this knowledge and these skills to pupils[15]. The developments are moving ahead far too quickly or are too complex.

Pupils are often well aware of how digital resources work, but are oblivious or hardly aware of the risks associated with the use of the digital resources and the consequences if digital resources are used for the wrong purpose[16]. Making just one mistake can often cause problems in the future. Pupils need guidance, therefore, but are still living in a different digital world than that of the school board members, teachers, and parents.

In summary, it can be said that the school environment lacks insight and awareness when it comes to cybersecurity. We see a challenge for educating the pupil of the 21st century. How should schools (school board members and teachers) ensure that they themselves become more cyber aware? How can they best guide the pupils in this respect? How can a connection be found between these two worlds?

Digital security in the 21st-century school

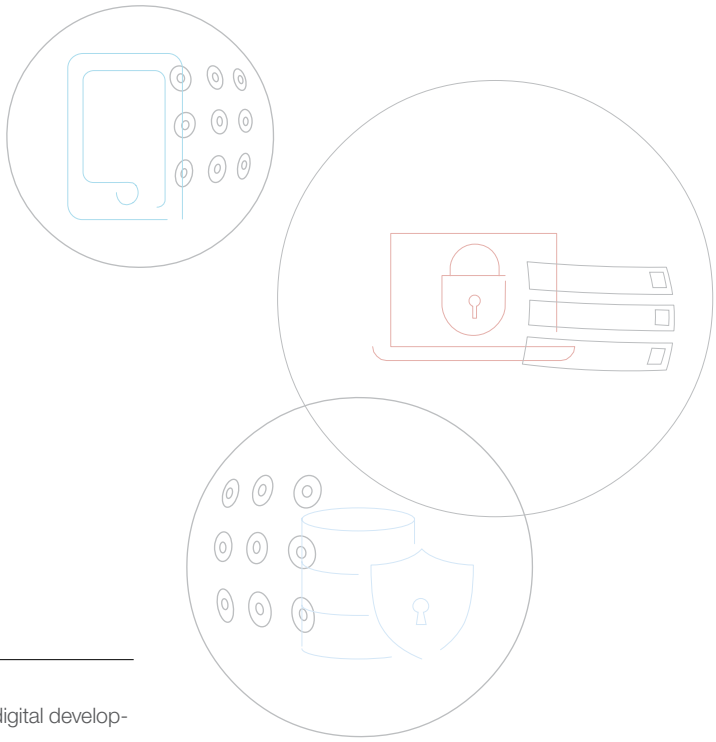
The pupil is the focus of the school. When it comes to the topic of digital security, the pupil is both the user and the professional of the future. Not only as possible specialists in cybersecurity, but also as cyber-aware users in other fields of expertise. In giving digital security a fundamental place in the school environment and within education, we see an important role for school board members and teachers. They can influence and further organize the school environment.

Increased awareness is essential to be able to organize digital security. This can be achieved via a mix of initiatives and activities in cooperation with the pupil; for example, by using the pupil's rapid adoption of digitization in education and for the security of the organization itself. Schools would be wise to take new trends and developments among young people seriously and to discuss these in the various classes. Teachers come

across a great many digital developments in practice in their classrooms. The perfect combination would involve organizing increased awareness by working together with pupils and also deploying their knowledge. Embarking on a “journey of discovery” together with the pupil can mean that the roles of teacher and pupil may be reversed from time to time in this context. Of course, both time and autonomy must be created for this by the school board, which is responsible for ensuring teaching time, learning lines, and training time for teachers.

It is also essential that the school environment itself set a good example. This means that the school and its school board members must become thoroughly familiar with the risks and measures. The starting point is that they must start thinking about the organization of digital security within the school. How equipped is the organization for this? What essential processes or data do I want to protect? A cybersecurity scan of the technical and organizational measures is one of the recommendations, as is the identification of risks. Based on these elements, an action plan can be prepared to achieve a structurally digitally secure school.

Finally, it is necessary for the school to be clear on what dependencies there are outside the school environment. Having one’s own affairs in order is not even enough these days. Educational tools and pupil administration systems are linked to the school environment. Vulnerabilities and threats from one chain party can have consequences for another chain party. Cooperation makes it easier to quickly anticipate new developments in the chain. The drafting and signing of a cyber covenant between the chain partners is a good first step in raising awareness in the chain. This could, first of all, include agreements on technical security aspects against cyber threats, in addition to agreeing on what risks and measures need to be tackled jointly in the chain.



[1]Frankwatching.com, December 2015: The three biggest digital developments for 2016.
[2]This article focuses on secondary education and vocational education.
[3]Siononderwijs.nl: registration and deregistration.
[4]Kennisnet, four in balance monitor 2013. The current status of ICT and education.
[5]Kennisnet, November 2013: Digital testing in secondary education.
[6]Kennisnet, vier in balans monitor 2015; CPS.nl, August 2015: knowing what works with ICT in education: five important insights from the Kennisnet conference.
[7]encrypts computer files so that they can no longer be opened.
[8]Security.nl, 21/02/2016: US school agrees to pay 8,500 dollars to ransomware.
[9]Metronieuws.nl, April 2015: Millions in damage for school because of cyber crime.
[10]Kennisnet, vier in balans monitor 2015; CPS.nl, August 2015: knowing what works with ICT in education: five important insights from the Kennisnet conference.
[11]Voogt & Pareja Roblin, 2010.
[12]Mijn-gemeente.com, March 205: Personal development important in digitization of society.
[13]Mediawijzer.nl, teaching material.
[14]PWC: lack of cyber expertise makes organizations extra vulnerable.
[15]Kennisnet, vier in balans monitor 2015.
[16]This picture is confirmed by the Cyber Security Council (CSR) in its "advice on cybersecurity in education and the business sector."

Conclusion

In summary, it can be said that the school environment is constantly changing and becoming increasingly digital. Along with the advantages, this also has a flipside: threats and vulnerabilities will only increase. Conscious attention to cybersecurity is essential for a safe school environment. The necessary efforts will have to be made in order to arrive at the desired level of awareness. The school board member and teacher have an important role in this and do not need to do this alone: use the knowledge and expertise in your own school environment.

About the authors

Evelien van Zuidam, MSc, is a senior consultant at Capgemini. With a background in criminology, she focuses on transformation issues relating to cybersecurity and crisis management. Martine Middelveld, MSc, is a security and privacy consultant at Capgemini Consulting. She is specialized in solving privacy issues and specifically in how organizations can set up compliance with the requirement to report data breaches.

For more information, you can contact the authors at:
evelien.van.zuidam@capgemini.com and martine.middelveld@capgemini.com

Integrate cybersecurity in regular management processes

Is cyber defense indeed thoroughly ingrained in the design, construction, breakdown, and maintenance processes of our critical infrastructure?

As a technical automation manager for part of the critical Dutch infrastructure, you want to be sure that cybersecurity definitely has a place in the day-to-day course of affairs. How do you make sure this is the case and manage to be "in control" by means of the activities directed at this?

Highlights

- Cybersecurity must be given a place in the management processes of our critical infrastructure.
- Calculate the work load and additional services for cybersecurity and reserve a budget for this. Use the tools and approaches that are available to get a view on the volume of work.
- Invest in an improvement program to get cyber defense procedurally embedded - and operationally scheduled.
- The maintenance engineers from "control and instrumentation" must learn the "Getting Things Done" (GTD) approach. This works for the existing, non-security-oriented work as well.

How do you explain to the management team how much extra effort must be put into cyber defense daily? How do you organize this new work? Everything that is designed to make our work easier, like mobile devices, cloud solutions, or even the remote control, entails security risks. In order to support the professional on the front line in defending critical infrastructure, we provide a few tools below which can be used in operational plans and checklists.

In 2009, the attention to cybersecurity in critical infrastructure sectors increased enormously as a result of the discovery of the Stuxnet virus, which was developed to sabotage Iranian centrifuges used for the nuclear program. Nuclear installations are vital infrastructure and this discovery boosted the development of the cybersecurity field, in addition to the attention that has traditionally been focused on physical safety.

With cybersecurity, the scope has been expanded for the security of the critical infrastructure, which has fortunately not suffered as many large-scale incidents. The security culture relating to the physical safety of vital infrastructure does not yet seem to be there for cybersecurity. If a fatal airplane disaster occurs, for instance, all the hairline cracks in the suspension bolts of 747 planes are inspected and replaced if necessary. Another example is the unbridled attention devoted to preventing excavation damage to the infrastructure on Dutch soil. An entire system of management measures was introduced for this, where excavation damage is still considered in the top 10 disruptors to the communication, electricity, and gas networks. A great deal of cybersecurity-related work has fallen to people who have a role in ensuring our vital infrastructure remains available. This article talks about how they can deal with this.

Imagine you are responsible for the technical automation of a particular area of the critical infrastructure, such as power plants,

rail infrastructure, runways, traffic lights, bridges, water, and energy distribution networks, and over the past five years you have taken steps to get a handle on cybersecurity. You inevitably reach a phase in which you emerge from your "fleet protection program" in which the dykes have been raised, the dyke warden has been appointed, and the major catch-up operation has been completed. In security terms, this is called realizing the first baseline security level.

Knowing that the cybersecurity domain is developing at a rapid pace, and realizing that defending infrastructure often costs a great deal more than what cyber attackers need to invest, you start to doubt whether you can indeed conclude the defense program or if you must arrive at a more permanent organizational form in which you can set up your defense very adaptively.

Below is an arbitrarily chosen list to offer an example of all the new work you will need to consider as the person responsible for the technical automation:

- When purchasing new assets, pay much closer attention to the security aspects.
- Conduct drills for defending the assets in the event of a cyber attack.
- Set up and monitor malware protection services.
- Where possible, perform penetration tests.
- If possible to do responsibly, operationalize patch management.
- Analyze history of deviating network traffic.
- Go through the security controls for proper functioning.
- Ensure professional support for remote access, including controls and procedures for working remotely in your control systems.
- Confront external engineers who come on site about the use of USB sticks and connections they make from their laptops to the process automation systems.

Some of the tasks cannot be carried out by the organization's own employees, but can best be performed by others. They must, in that case, report on how matters stand. It comes down to setting cyber defense goals, getting the cybersecurity work done, evaluating how it runs, constantly brushing up on knowledge, working with other employees, and keeping an overview of the situation.

What are some resources on which you can base your operational plans? A good example is a practical security guideline that the Norwegian government drafted for the expansive oil and gas industry there, named OLF104, which provides a good guideline in 16 simply-formulated questions[1]. Another example is the US Department of Homeland Security, which has developed a complete "security assessment tool" that helps translate risks into the security measures to be taken[2]. It has also set up a specific training for the security of control systems which simulates an actual physical process having to be defended by half of the participants, while the other half of the participants attack. A last example comes from the German government, which has required businesses in vital sectors to also include the technical automation in the Information Security Management System (ISMS), so that regular periodic cybersecurity activities are on the agenda and can therefore be performed on time (such as audits, for instance).

These are all examples of ensuring that there is insight into the performance of cybersecurity work, knowing how well-equipped you are, determining what matters can be taken care of internally

(by the IT department), and what needs to be outsourced and what matters need to be embedded in existing operational procedures and working methods. An example is the Management of Change (MoC) approach for changes in a plant or physical processes. The security aspect still does not usually appear in this (though the IT aspect often does), but this should indeed be added so that it can then be consistently implemented in all changes.

The operational improvement approach is usually based on a Plan-Do-Check-Act (PDCA) cycle. The operational maintenance approach is often based on urgent and non-urgent maintenance orders to be scheduled. It is a good idea to also use these existing approaches for cybersecurity-related work and therefore to add scheduled maintenance for the performance checks of log files, the viewing of virus scanner statistics, and the performance of system patches. If a larger overhaul of an installation or change is to be implemented in the process, the major security improvements should also be implemented, and therefore be scheduled along with the other work with adequate priority. Time must also be reserved for matters that fall under the broad category of "cooperation and coordination". This could include regular consultation with suppliers to discuss (policy) changes on both sides, with respect to impact and responsibilities, to discuss the current state of affairs, and to look back on the changes that have been implemented. The coordination discussions with the internal IT department in which the security standard should be put on the agenda could also be thought of here.

The most difficult point to deal with is the constant flow of new security vulnerabilities. These must not be neglected, but are very diverse in terms of impact, approach, and lead time. Just like some other types of maintenance, these can be classified as "urgent". Generally these urgent maintenance orders do not come from the control room of a factory or power plant, but from the monitoring security dyke (from the security operating center or computer emergency response team of one of the suppliers, for instance). It is important to then discuss this with the supervisor and make it into an urgent order.

Another important aspect is encouraging security awareness. This encompasses conduct that sets an example and holding regular special awareness-raising campaigns as well as confronting others if work is being performed in a way that is not secure. Only use secure file exchange or no file exchange at all must become as commonplace as holding the railing when taking the stairs. Holding regular drills on how to act in the event of a cyber attack must also be regularized. This is similar to a regular crisis management exercise, but then with a special focus (scenario) on the invisible danger of cyber crime.

[1]https://www.norskoljeoggass.no/en/Publica/Guidelines/Integrated-operations/104-Recommended-guidelines-for-information-securitybaseline-requirements-for-process-control-safety-and-support-ICT-systems/.
[2]https://ics-cert.us-cert.gov/Assessments

Conclusion

The battle between cyber defense and attack continues unabated. In the long term, product suppliers of technical automation will have mastered "security by design" and the number of common vulnerabilities will decrease significantly. Unfortunately, this will not eliminate the problem, but simply shift to more advanced vulnerabilities. It is important to embed cyber defense in your organization's regular security management, on the basis of a risk-based approach.

About the authors

Christiaan van Essen, BBA, is a consultant at Capgemini. Christiaan mainly performs assignments in the public market and is an expert in the area of security management. Milé Buurmeijer is a senior ICT architect at Capgemini and has broad experience in protecting critical infrastructure with the increasing digitization of the primary processes. Roger Wannee is a principal consultant at Capgemini and as such is active in the area of public order and security. He focuses specifically on issues in the areas of cybersecurity, crisis management, policy realization, and business operations.

For more information, you can contact the authors at:
christiaan.van.essen@capgemini.com,
mile.buurmeijer@capgemini.com and roger.wannee@capgemini.com



The Chief Information Security Officer in 2016

New challenges demand new competences

With the constant flow of new threats and changing legislation, the role of the Chief Information Security Officer (CISO) is changing as well.

Highlights

- The CISO is being given an increasingly important role.
- The evolution of digital threats brings new challenges.
- The CISO's competence profile is changing accordingly.
- In practice, three types of CISOs can be distinguished.

Traditional role in the organization

The CISO's job is to formulate the information security strategy of his organization and establish a security organization. He is responsible for implementing information security measures in the organization and providing direction for both the policy and execution. In practice, however, the CISO is still often operationally involved in the technical aspects of cybersecurity. Beyond that, the CISO's responsibilities do not seem to be keeping pace with his mandate and budget. If things go wrong, he is viewed critically, but he is seldom given the powers or resources to get things in order and implement preventative measures. His role is primarily an advisory one.

The position of the CISO also differs significantly per organization. In some cases he reports to the CIO, in others to the CFO. Only sporadically he reports directly to the CEO, which should be his rightful position, given the increasing importance of his role. In the event of major breaches of company data or

systems, the consequences for the organization can be enormous, and it must be possible to quickly change gear in respect to aspects that reach far beyond IT.

Boardroom

Fortunately information security is high on the agenda in many boardrooms these days. The many reports on cyber crime in the media have contributed to this significantly. While cybersecurity used to be seen mainly as a cost item, directors now realize that critical business processes are exposed to real danger if data and systems are not adequately secured. This means that the CISO's role must be expanded from the realm of technology to that of business, and even to legislation and regulation in this area.

One of the challenges is that security measures internally are often perceived as difficult: "Security is getting in the way of our ambitions". That presents a new task for the CISO. Together with the business, he must find a balance between adequate securing of information and sufficient freedom of movement for employees and clients. He cannot avoid accepting certain risks in this process. "Bring your own device," the "Internet of Things," and other innovative techniques all increase the risk of data breaches. At the same time, they also provide the organization with important advantages. No one will deny the risks of social media, cloud services, and mobile devices which give users access to company or personal information. Excluding these resources, however, has long ceased to be an option, of course.

On the other hand, cyber attacks are becoming increasingly advanced and progressively more targeted. The CISO must therefore receive a constant feed of the current threats and be able to immediately assess the impact of these on the organization. Setting up a properly functioning ISMS and incident response plan is therefore one of the CISO's new and more important tasks.

Competence profiles

The expanding security landscape and changing role of the CISO in the organization demand additional and different competences. The CISO will have to be able to let go of his traditional IT focus and enter consultation with the business about cybersecurity: a process of give and take based on understanding of each other's objectives. That imposes demands on the CISO's communication skills, his emphatic ability and his firmness in daring to make decisions. Supported by specific experts, he will constantly have to be up-to-date on the latest technological developments and legislation in order to then work together with the business to translate these into adequate and accepted compliance and security measures. He will also have to be able

to convincingly advise the management on security, based on a clear vision and strategic insight, and ensure good security awareness among all employees in the organization. And he will also have to join sector consultations with other CISOs. In short, the CISO will have to have a much broader competence profile than in the past, because a great deal more will be expected of him.

In practice, we see different types of CISO

The network specialist/technician

This CISO has a degree in technology or computer science, usually started his career in IT, and specialized in security later on. This type of CISO often puts the focus on the technology and has difficulty writing strategic and policy memos. It is very important for this CISO to achieve CISM (Chief Information Security Manager) certification in order to get a better understanding of the governance. In small organizations, this CISO really reaches his full potential, because he also has the opportunity to lend a helping hand himself.

Legal expert/policy advisor

Many CISOs have grown into the role from a position as legal expert or policy advisor. This type of CISO often has a good relationship with the management, has strong communication skills and considers compliance a priority. In contrast to the technical CISO, this CISO will have more difficulty with the practice and the technology. Achieving the CISSP and CEH certificate offers a solution for gaining a better understanding of digital threats. This type of CISO is ideal for large organizations with their own security departments.

Police officer/military

These CISOs started their career in the military or law enforcement and have acquired their technical expertise through "on-the-job" learning. They are at their best in hierarchical organizations. A pitfall for this type of CISO is that they often put too much focus on the physical security and do not pay enough attention to digital threats.

What type of CISO is the most suitable depends on, among other things, the size and strategic objectives of the organization. For the ideal CISO, an organization will have to look for a genuine all-rounder with a good deal of experience and a combination of the above profiles. He must be able to bring together opposing interests, and in doing so be able to assess the value of advice from different experts and the interests of the management. It goes without saying that the greater responsibility on the part of the CISO should also be accompanied by a greater mandate to be able to take decisive action when necessary.

Conclusion

Owing to the rapid technological, social, and legal developments in relation to cybersecurity, the job responsibilities of the CISO are becoming broader, more complex, and more important. This calls for very different competences. It is therefore a good idea to critically evaluate the position and job requirements of the CISO and in doing so contribute to a good and balanced securing of systems and data, which is appropriate to the nature of the business, compliant with legislation and regulations, and broadly supported by the business.

About the authors

Guido Voorendt is a cybersecurity consultant at Capgemini. He is active in the domain of public order and security and specialized in security governance, phishing, privacy and identity and access management. Matthijs Ros is a managing consultant at Capgemini. He is active in the domain of public order and security and, as security leader, manages the cybersecurity team of Capgemini Nederland.

For more information, you can contact the authors at:
guido.voorendt@capgemini.com and matthijs.ros@capgemini.com
@gvoorendt and @matthijsros

colophon

Capgemini Nederland B.V.
P.O. Box - 3500 GN Utrecht
Tel. +31 30 689 00 00
www.capgemini.com/cybersecurity

Advice, design and production: Marketing & Communication: Nicole Hartung, Joke Achterberg and Ashim Karmakar

Photography: Sujoy Karmakar, Shutterstock

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Capgemini Consulting

About Capgemini

With more than 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

With over 2,500 professional employees, we offer a complete range of integrated cybersecurity services to guide and secure the digital transformation of companies and administrations. We protect your data, IT and industrial systems, and the Internet of Things (IoT). We have the resources to strengthen your defenses, optimize your investments and control your risks. They include our security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and our R&D team that specializes in malware analysis and forensics. We have ethical hackers, eight security operation centers (SOC) around the world, a licensed Information Technology Security Evaluation Facility, and are a global leader in the field of testing.

Read more on
www.nl.capgemini.com/cybersecurity &
www.capgemini.com/cybersecurity