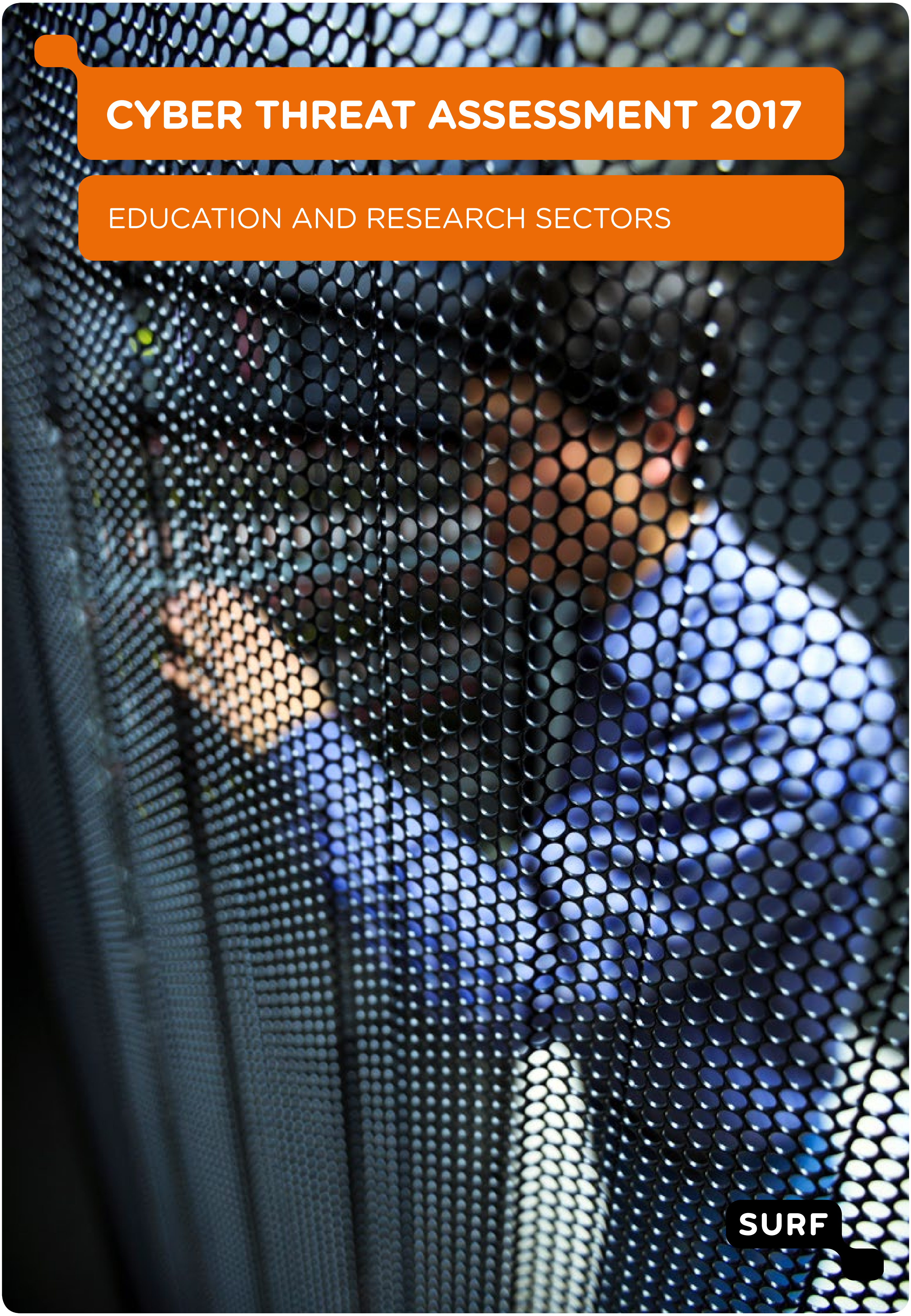
CYBER THREAT ASSESSMENT 2017

EDUCATION AND RESEARCH SECTORS



SURF

TABLE OF CONTENTS

PREFACE

As digitisation continues apace in the Netherlands – and consequently in Dutch education and research – we are now seeing unprecedented opportunities to reform the education system. New forms of learning heavily depend on safe and reliable ICT. However, this makes us vulnerable to attacks as well. Last year was characterised by denial-of-service attacks – facilitated by the Internet of Things devices – and a huge increase in ransomware attacks that, in some cases, caused substantial damage.

The most striking example was the ransomware attack at the Danish multinational Maersk. As a result, no ships could be loaded or unloaded for several days at its sister company APM Terminals in Rotterdam. Maersk estimates the financial damage to be several hundred million dollars, and it took a month before the company was fully operational again. Therefore it is imperative that companies are aware of the various threats, that they take measures to combat these threats in good time, and that they are able to respond quickly if a threat does materialise.

The SURF communities SCIRT and SCIPR offer a fantastic platform for the exchange of information, quickly making organisations aware of any problems encountered by their counterparts. Up to now, there have been few problems caused by ransomware in the education and research sectors. However, the extensive distribution of this type of malware and the increase in the number of variations make it necessary to remain alert as to its existence, and to develop more automated methods of being able to quickly share information about threats.

Privacy protection is more prominent than ever before. At the beginning of 2016, in the Netherlands it became mandatory to report data leaks. The Dutch Data Protection Authority can now impose fines on anyone who fails to comply with this notification obligation. Furthermore, the General Data Protection Regulation is set to enter into effect on 25 May 2018, making personal data protection requirements even stricter and increasing the fines that may be imposed. It would be unwise to underestimate its potential impact. SURF offers a number of resources to help organisations meet the requirements set by the GDPR, and several collaboration initiatives exist. According to intelligence services, espionage by both states and criminal organisations is an ever-increasing problem. Here, too, it is important for organisations to be aware of the possibility of sensitive information being stolen. They also need to be aware of what is happening in their IT environment and take effective measures accordingly.

This report sets out the developments that took place between October 2016 and October 2017, and describes the effect they had on the most relevant threats to education and research organisations. The report shows that we are making progress in information security, but that at the same time we are facing new challenges, such as the increase in the number of Internet of Things devices, the increasing digitisation of students, teachers, researchers and other staff in organisations, and the substantial increase in espionage by both criminals and state actors.

Erik Fledderus
General Manager SURF

Marjolein Jansen
Vice Chairman Vrije Universiteit Amsterdam
and Ambassador for Cyber Security SURF

SUMMARY

This Cyber Threat Assessment report gives managers and security officers working in education and research a clear idea of the developments on which they should focus to improve their information security and privacy protection. During the research period (October 2016 to October 2017), we charted developments that influence the threat assessment for education and research. It concerns the following developments:

Criminals and state actors continue to constitute the greatest threat and cause the most damage. According to the NCSC and intelligence agencies, the threat of digital espionage remains at a high level, and other states use such means to try to siphon off information.

The vulnerability of the Internet of Things (IoT) has led to disruptive attacks that clearly illustrate the need for digital resilience to be strengthened. The number of IoT devices is set to increase sharply in coming years, potentially reaching a total of 75 billion devices worldwide by 2025. Many of those devices will have vulnerabilities that are secured insufficiently and, in many cases, cannot be patched.

Resilience of individuals and organisations cannot keep up with the proliferation of the threats. In general, resilience in Dutch organisations is poor, and recent incidents have shown that the impact of such incidents can be huge. Resilience in education and research sectors seems to be better organised.

The increasing digitisation of citizens (and therefore of students, teachers, researchers and other staff at education and research institutions) is changing the threat landscape. Students, teachers, researchers and other staff at institutions are increasingly making use of mobile devices – in many cases their own smartphones or tablets (BYOD). This is blurring the boundaries between private and company information and making it more difficult to monitor improper access to critical data. When the General Data Protection Regulation enters into effect in mid-2018, organisations will have to put processes in place for the protection of personal data, and the notification of incidents.

Denial-of-service attacks will continue, but can be kept under control. SURFcert statistics indicate that denial-of-service attacks will continue unabated. It appears that, given their noticeable decrease during holiday periods, many attacks are carried out by students. Together with the organisations concerned, SURFnet has developed adequate solutions to mitigate these attacks, thereby limiting the impact.

Malicious parties are still taking advantage of vulnerabilities, including on mobile devices, to gain access to critical systems. Many vulnerabilities, including zero-day vulnerabilities, are either not patched or patched too late. This gives malicious parties ample opportunity to carry out attacks that are difficult to detect.

Education and research institutions are collaborating in all sorts of ways to increase their resilience together as a means of responding to these developments. In the SURF communities SCIRT and SCIPR, a great deal of information is exchanged, allowing organisations to learn from each other. Other SURF services such as Cybersave Yourself, SURFaudit and SURFcert are also available to help organisations improve their information security.

Attackers

There are many different types of attackers, ranging from script kiddies to professional criminals and state actors. Each type of attacker has certain skills and their own motives for carrying out attacks. That means that harmless attacks by, for example, script kiddies, are simply annoying, while attacks by criminals cause substantial damage. Since the advanced attacks carried out by professional criminals and state actors are particularly difficult to detect, organisations need to mobilise advanced resources to defend themselves against them.

Type of threat	**Manifestation of the threat**	**Risk level**		
Type of threat	Incident	Education	Research	Operations
1. Obtaining and publicizing data	• Research data is stolen • Privacy data is leaked and published • Blueprint of position of research institutions falls in the wrong hands • Fraud by obtaining exam and exercise data	MEDIUM	HIGH	MEDIUM
2. Identity fraud	• Student has someone else take his/her exam • Student impersonates another student or teacher to obtain exams • Activist poses as a researcher • Student impersonates a teacher or employee to manipulate study results	HIGH	MEDIUM	LOW
3. Disruption of ICT	• DDoS-attack shuts down IT-infrastructure • Critical research data or exam data is destroyed • Setup of research institutions is sabotaged • Educational resources are unusable because of malware (e.g. eLearning or the network)	MEDIUM	MEDIUM	MEDIUM
4. Manipulation of digitally stored data	• Study results are tampered with • Research data is manipulated • Operational data is tapped	HIGH	LOW	LOW
5. Espionage	• Research data is tapped • Intellectual property is stolen through a third party • Foreign students under control of foreign state	LOW	HIGH	LOW
6. Taking over and abusing ICT	• Setup of research institution copied • Systems or accounts misused for other purposes (botnet, mining, spam)	LOW	MEDIUM	MEDIUM
7. Knowledge damaging reputation	• Web site compromised • Social media account hacked	LOW	LOW	LOW

Table 1: Relevant threats to education and research institutions

TERMINOLOGY

100 GE 100 Gigabit Ethernet connection, e.g. on the AMS-IX or with an internet provider such as KPN or Ziggo.

Actor The individual or group responsible for a malicious incident.

AMS-IX The Amsterdam Internet Exchange – the major internet hub in the Netherlands and one of the largest internet hubs in the world. Virtually all internet traffic with foreign countries runs through the AMS-IX.

AVG General Data Protection Regulation (GDPR) EU 2016/679 This replacement of the Dutch Personal Data Protection Act has been in force in the Netherlands since 2016, but will enter into effect in all EU countries from 25 May 2018.

Awareness A general term used to indicate the extent to which a person or organisation is aware of the security risks and of which measures are needed to combat said risks.

Big data Large amounts of data, which are received on a large scale and stored in an unstructured fashion, and which demand cost-effective, innovative forms of information processing that enable enhanced insight, decision-making and process automation (Gartner).

Botnet A collection of software robots that can act automatically and independently, usually with malicious intent. The botnet is driven by what are known as Command & Control (C&C or C2) servers.

Cryptoware Ransomware that encrypts files, so they can no longer be opened.

DDoS Distributed Denial of Service. A denial-of-service attack, where multiple computers (such as a botnet) render a system or web application unavailable to users.

Drive-by download A download that takes place unnoticed, often automated, during a visit to a website, The aim is to install malware on the victim's computer.

Dyn A company that supplies DNS management services. Has been a subsidiary of Oracle since 2016.

IoT Internet of Things. A concept where everyday devices such as video cameras, washing machines and refrigerators are connected to the Internet, can communicate with each other and operate with a certain degree of autonomy.

Jaff Ransomware that is spread through phishing or spam messages. It distinguishes itself from other ransomware variants by the high ransom demanded (2 bitcoins = more than EUR 10,600 on 31 October 2017).

Malware Malicious software used to disrupt a computer system deliberately. The aim varies from making the system unusable to collecting information.

Mirai Malicious software that infects IoT devices and incorporates them in a botnet.

NCSC	The Dutch National Cyber Security Centre of the Ministry of Justice and Security. This is the central information hub and centre of expertise for cyber security in the Netherlands. The NCSC's mission is to contribute to improving the resilience of Dutch society in the digital domain and to ensure a safe, open and stable information society.
Petya	A cryptoware family that targets Windows systems. Once contaminated, the file system is encrypted.
Phishing	A form of Internet fraud that aims to get a user to divulge information, for instance login information or bank details. The fraudster pretends to be a trustworthy person or organisation in order to mislead the victim.
Ransomware	Malicious software (malware) that blocks a computer system until a ransom is paid.
Serpent	Cryptoware that is distributed by phishing or spam messages. Once contaminated, files are encrypted with a strong encryption algorithm. Serpent distinguishes itself from other cryptoware in that the ransom is increased if not paid within 7 days.
Spam	Unwanted electronic mail that distributes advertisements or aims to tempt the recipients into visiting a certain website (often malicious).
State actor	The individual or group responsible for a malicious incident carried out on behalf of a state. This is often a domestic, or foreign, intelligence agency.
Wannacry	Ransomware for Windows systems. It is distributed through phishing emails and via a vulnerability in the Windows operating system (EternalBlue).
Zero-day vulnerability	Vulnerability in software that has not been discovered yet, or for which there is no security update available as of yet.

1. INTRODUCTION

In the previous editions of the 'Cyber Threat Analysis – education and research sector', we defined seven types of threats that affect education, research and management processes at universities, universities of applied sciences and colleges (see table 1, page 5).

These threats still exist. In particular, *identity fraud and manipulation of digitally-stored data* are types of threats that can negatively impact the education process severely, while Obtain*ing and making data public* and *Espionage* can have the most negative effect on the research process. The negative effects of *Obtaining and making data public* also apply to business management.

However, we have established that all education and research institutions are making progress when it comes to information security, further improvements are being considered on all manner of forums, and steps are being taken to tackle this together.

This edition builds on earlier editions of the Cyber Threat Assessment report, but emphasises the developments that have taken place in the recent period (October 2016 to October 2017) along with the effects they have on education and research. These developments have been charted based on interviews with security officers at organisations, and the information emerging from the SCIRT and SCIPR communities. Various public sources were also consulted.

This helps managers of organisations and security officers being aware of developments on which to focus in order to improve their information security and privacy protection.

Developments

On 21 June 2017, the Dutch National Coordinator for Counter-terrorism and Security (NCTV) presented the Cyber Security Assessment Netherlands 2017 to the Dutch House of Representatives and offered the telling conclusion: “Digital resilience in the Netherlands is lagging behind the increasing threat” [1]. The report lists five core findings that affect Dutch society, of which the following especially affect the education and research sectors.

- Professional criminals and state actors continue to be the most significant threat and inflict the most damage.
- The vulnerability of the Internet of Things has resulted in disruptive attacks that endorse the need to enhance digital resilience.
- The resilience of individuals and organisations is lagging behind the increasing threat.

These developments are discussed in Chapters 2, 3 and 4 respectively.

Society is digitising increasingly [2] as exemplified by the Internet of Things, big data, social media, digital learning environments and the growing number of mobile devices and their increasing capabilities. This is examined more closely in Chapter 5.

Statistics from SURFcert and various publications show that denial-of-service attacks are an ongoing problem. We also continue to see a significant drop in the number of alerts during the holiday periods. We will look at this development more closely in Chapter 6.

Vulnerabilities are evident in all types of software. Generally, when a software supplier discovers a leak in their product, they issue a patch. However, there are vulnerabilities that have already been discovered, but are not yet known to the supplier (zero-day vulnerability). Chapter 7 focuses on this development.

Attackers

Chapter 8 is the concluding chapter, in which we will discuss the various actors involved in attacks, their skills and motives, and the types of threat that they influence.

2. CRIME AND ESPIONAGE ON THE RISE

Rapid development

Publications by the AIVD, MIVD [4] and NCSC [1] intelligence agencies show that criminals and state actors constitute the main threat to Dutch digital security, and that they are developing more quickly than other actors.

Ransomware

Professional criminals frequently use ransomware, and educational institutions are among their targets. This was demonstrated by various ransomware attacks that took place at educational institutions during the research period [source: SCIRT [5] mailing list]. Among the types of ransomware detected were Wannacry, Petya, Jaff and Serpent; some of these can move throughout the entire network once they have infiltrated it, which means that the contamination of a single machine is enough to infect an entire network [6]. The initial contamination can be caused by a phishing or spam mail. Phishing mails in particular have become more and more difficult to distinguish from a regular email, increasing the likelihood of one system being contaminated. The use of so-called drive-by downloads has not stopped either. During a visit to a regular website, malware is downloaded unnoticed (and fully automated) or the user is diverted to a website controlled by the criminals.

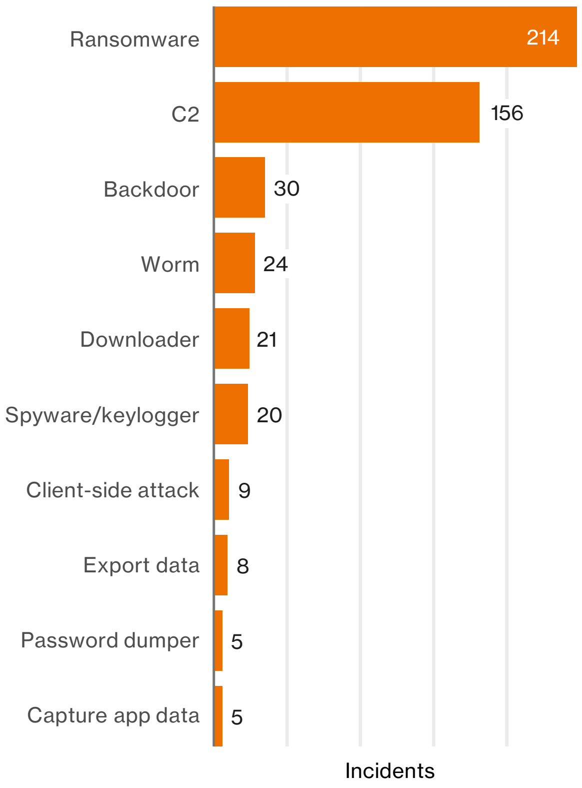


Figure 1: The most common malware in cyber incidents (source: Verizon – DBIR 2017 [38])

Digital espionage

The AIVD's 2016 Annual Report [7] indicates that the threat of digital espionage remains high, and that other states use it to try to siphon off information. This was already mentioned in the AIVD's [8] 2015 Annual Report: "The AIVD acknowledged a record number of cyber espionage attacks carried out on Dutch government departments." China, Iran and Russia are named as the major state actors, with the AIVD confirming that the attackers were searching for extremely specialised and sometimes even experimental technology that has yet to prove its market value. Not mentioned in the AIVD reports are intelligence services in the US and other western powers [9] that are just as happy to make use of all the internet offers as a means of gathering information from hostile states and allies alike.

Political, military and economic motives

The motives of state actors (intelligence services) are not limited to exerting political influence or obtaining information about military or state secrets. Economic motives play an important role as well. By obtaining secret information (also from businesses) and intellectual property, countries can achieve a competitive advantage without having to make major investments, for example, in research in their own countries.

"Possession of valuable information in the fields of technology and science allows foreign states to reduce their dependence on knowledge and products from abroad. This means they can improve their economic competitiveness or geopolitical position of power, such as through the accelerated modernisation of their armed forces." [4]

Attacks that are hard to trace

State actors have many resources at their disposal as well as extensive knowledge and skills and their attacks can be difficult to trace. According to the AIVD/MIVD, businesses and institutions appear to have insufficient knowledge about how to arm themselves against cyber espionage [4], which is why cyber attacks are often successful. In addition, many organisations are not even aware they have become victims until they are alerted by a service such as an intelligence agency [10].

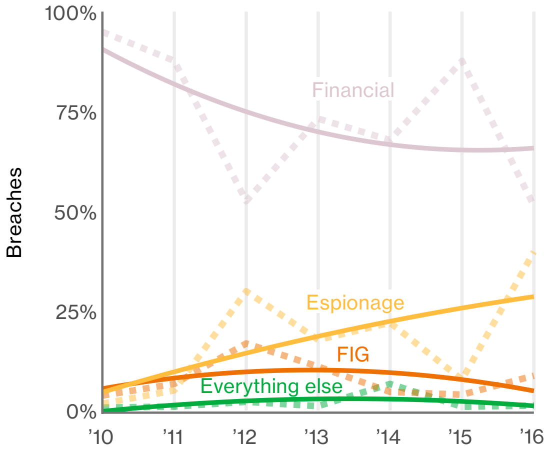


Figure 2: Motives of actors, where FIG stands for Fun, Ideology and Grudge (source: Verizon – DBIR 2017 [38])

Advanced infrastructure – an attractive transit port for attacks

Our country's well-developed ICT infrastructure continues to attract interest as a transit port for digital attacks. The AIVD has identified various state actors who misuse our infrastructure to conduct attacks on other countries. This means the Netherlands is involved in the spread of digital attacks that constitute a violation of the economic, military and political interests of other countries unintentionally [7]. Within the already well-developed ICT infrastructure in the Netherlands, SURFnet's own infrastructure is extremely well developed. It is linked directly by two 100 GbE ports to the AMS-IX, one of the largest Internet hubs in the world, making it an attractive target for various types of cyber criminals.

Conclusion

Reports by the AIVD and the MIVD show that professional criminals and state actors are active in all manner of organisations in the Netherlands. International reports support these findings. It is important to be prepared for this, and to make sure any signs indicating this kind of activity are recognised early on.

3. RISE AND GROWTH OF THE INTERNET OF THINGS

Major security problems

The number of IoT devices continues to grow, and will increase further in the coming years: from more than 20 billion in 2017 to an estimated 30+ billion in 2020, and in excess of 75 billion in 2025 [11] [12]. At the same time, there are huge security problems with IoT devices. They contain vulnerabilities that are rarely patched (if at all), and many of these devices are supplied with a hard-coded password or a default password that the user should change subsequently. However, most users either do not realise that they should have changed the password or do not know how to do so. Although there has been some talk about legally enforcing better security of IoT devices, or setting up a certification (similar to KEMA-KEUR or the CE marking), it is difficult to know how effective this would be in the current world market [13] [14] [15].

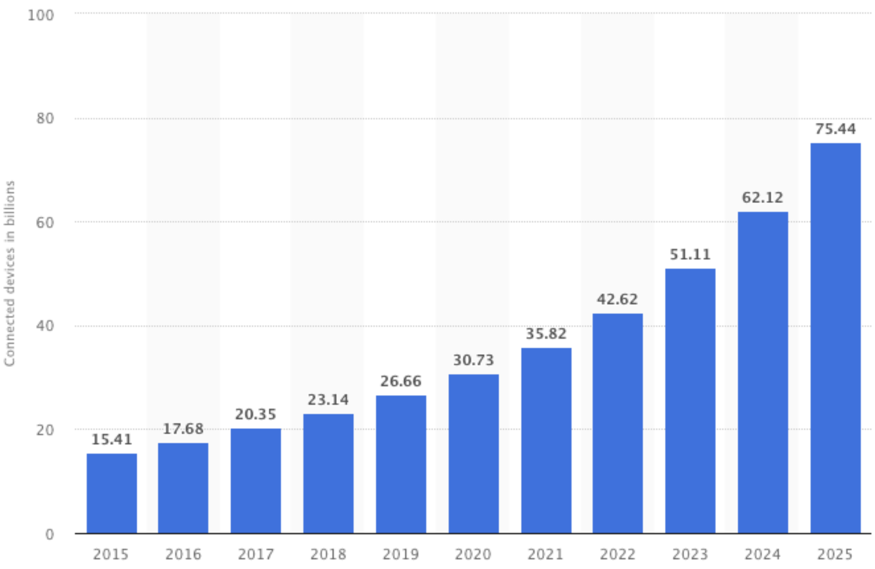


Figure 3: Expected increase in IoT devices worldwide up to 2025 (source: Statista)

Number of attacks doubled

Research carried out by Symantec [16] reveals that there were almost twice as many attacks on IoT devices in 2016 (in a test environment). In January, scans (a possible harbinger of an attack) were made of on average 4.6 unique IP addresses, increasing to 8.8 in December (see Figure 4).

IoT devices can be misused as components of a botnet, but can also serve as stepping stones to attack other systems in an internal network. Malicious parties can then steal personal information.

Additional vulnerability for IoT devices

As IoT devices are less secure than laptops, desktop systems or servers, it is easier for malicious parties to successfully attack them.

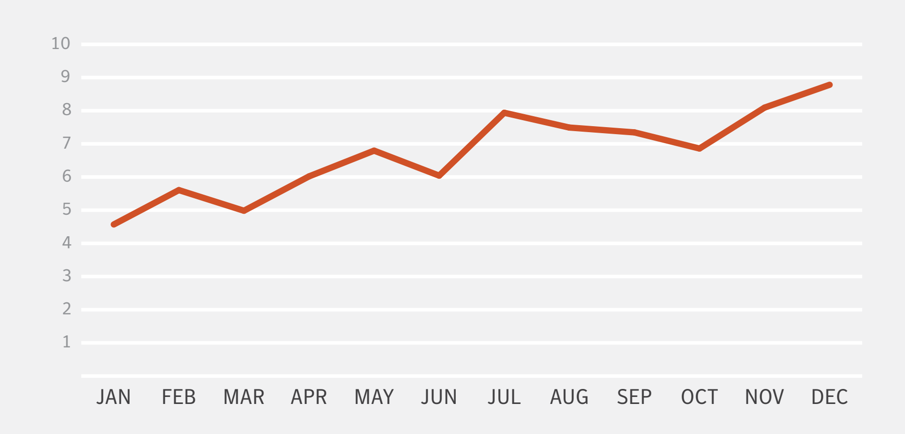


Figure 4: The number of attacks on IoT devices per hour (source: Symantec – ISTR 22)

Conclusion

A huge increase in the number of IoT devices is expected, while at the same time the number of attacks on IoT devices is increasing. Combined with the poor security of these devices as of yet, the threat landscape will change enormously, and organisations need to be prepared.

4. RESILIENCE IN EDUCATION AND RESEARCH IS GOOD

Collaboration required

Recent incidents have shown that in general resilience among Dutch organisations is poor and that such incidents can come at an extremely high financial cost [17] [18] [19] [20]. Increasing digitisation makes everyone vulnerable to cyber threats. This is why we need more collaboration between all parties concerned. The Cyber Security Council [24] and the Netherlands Scientific Council for Government Policy [22] both emphasise the importance of collaboration. In September 2017, the Minister of Economic Affairs, Henk Kamp, announced that a Digital Trust Centre will be set up in 2018 to help companies become more resilient to cyber threats [23]. The NCSC has also been coordinating the National Detection Network [24] for some time now. Its aim is to limit damage caused by digital hazards and avoid risks by sharing information about threats.

Cooperation has already been established at various levels among educational and research institutions affiliated with SURF. There are communities where information is exchanged, such as SCIRT (operational) [25] and SCIPR (policy) [25], along with services such as SURFcert [26], SURFaudit [27] and Cybersave Yourself [28], whose aim is to raise the standard of information security at institutions.

SURFcert statistics and discussions in the SCIRT community show that the resilience of education and research institutions is actually organised rather well. For example, in the event of a malware outbreak information is exchanged rapidly, so that other organisations not yet affected can take preventative measures.

More awareness needed

One of the findings of the SURFaudit benchmark 2015 [29] was that still much can be done in terms of information security awareness. For example, measure 7.2.2: “All employees of the organisation and, where relevant, contractors are provided with suitable awareness training and regular refresher courses on the organisation’s policy rules and procedures that are relevant for their work” from the standard of Information Security HO 2015 scored well below the baseline.

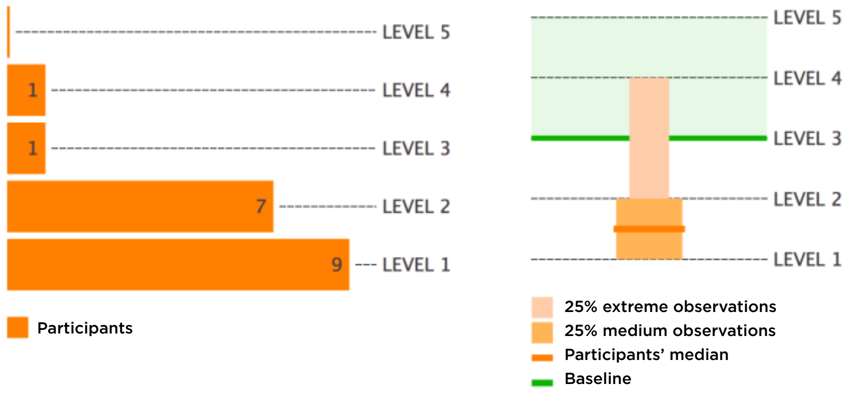


Figure 5: Detailed score from SURFaudit benchmark 2015 – measure 7.2.2

Conclusion

Educational and research institutions appear to be doing better in digital resilience than Dutch organisations in general. A number of collaborative partnerships have also been established in this sector that should increase resilience. However, it appears there is still room for improvement in educational and research institutions, particularly when it comes to awareness.

5. INCREASING DIGITISATION

Bring Your Own Device

Society is becoming increasingly dependent on digital information technology. We have now reached the point where every Dutch citizen has one or more devices that are more or less permanently connected to the Internet. Students, teachers, researchers and other employees at education and research institutions are increasingly using their own devices. This BYOD concept (Bring Your Own Device) makes it possible to connect their own devices to systems that may contain sensitive information.

Extra security for sensitive information

The challenge for institutions is to secure sensitive information effectively, only allowing access to authorised users, and to make sure such information is used correctly.

The following questions are important: how much and what kind of data should an institution be permitted to collect, how should that data be protected, for how long should data be stored (if at all), who is authorised to access data and for what purposes may the data be used?

All manner of initiatives are springing up, aimed at reconciling these seemingly conflicting demands. TNO, for example, is working on TrustTester [30] for the safe validation of personal information and the Privacy by Design Foundation [31] manages IRMA (I Reveal My Attributes), which aims to verify relevant properties of yourself to others in a privacy-friendly manner.

There are, however, potential complications (some of which are legal): who is responsible when a private device is lost or infected with a virus? For example, is the institution permitted to delete everything from the device to prevent sensitive information from being leaked?

Teachers, researchers and other staff may be able to deal with this by having the institution issue its own devices. The problem is much greater for students given that they, too, have access to sensitive information.

General Data Protection Regulation

New legislation has come into force that could potentially exacerbate the effects of information security problems. For example, on 1 January 2016 breach notification became mandatory, with a new supervising authority able to issue heavy fines as part of decisive action against offenders [32]. In Europe, the General Data Protection Regulation (Regulation (EU) 2016/679) came into force in 2016. In the Netherlands it will replace the Dutch Personal Data Protection Act (Wbp) on 25 May 2018, following a transition period of two years. In fact, the GDPR will then enter into effect in all EU member states, substantially raising the maximum fines. And additional organisational and technical measures will be required to effectively protect personal information.

All media attention surrounding the GDPR has resulted in privacy and information security becoming a major focal point for all governments, businesses and institutions. Organisations are now focusing on making proper preparations for 25 May 2018.

However, this legislation also further complicates information security: if personal information is leaked, the organisation is probably responsible, and can be fined heavily by the Autoriteit Persoonsgegevens (Dutch Data Protection Authority).

Figure 6: Here at SURF, we are also counting down to when the AVG comes into force (photo: 3 November 2017).

Conclusion

Protecting sensitive data is becoming an increasingly complex issue. This is because of the increasing use of private devices at educational and research institutions to access potentially sensitive information, and the mingling of personal and company data that comes with it. Moreover, the imminent arrival of the GDPR requires an approach to data protection that takes into account the specific requirements associated with personal information.

6. DENIAL-OF-SERVICE ATTACKS CONTINUE UNABATED

Consequences can be assessed

SURFcert data shows that although denial-of-service attacks are continuing unabated, the consequences can be properly dealt with. There has been no structural change in the total number of notifications registered with SURFcert. The average number of notifications per week was more than 50 in 2016, while the average in the same period for 2017 was just under 45. The consequences of all these notifications are minimal.

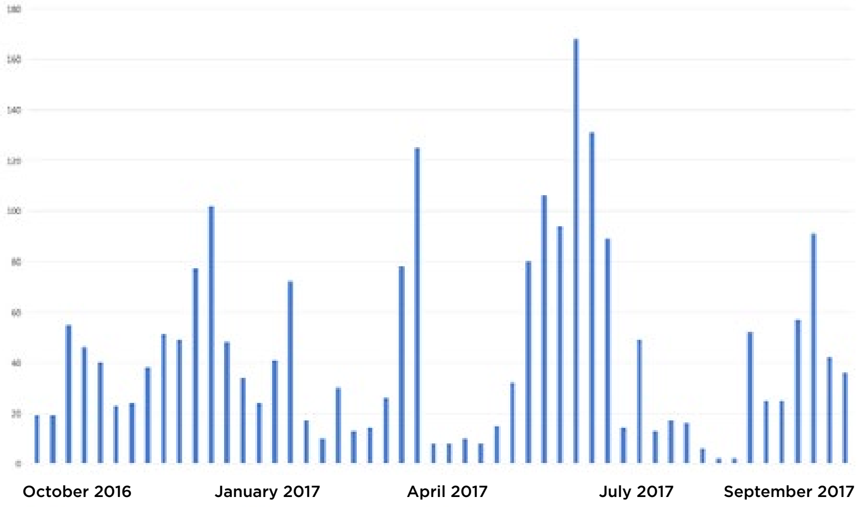


Figure 7: Number of DDoS notifications per week – source: SURFcert

Striking in the graph is that the months of April/May and July/August are noticeably quieter than the rest of the year. These periods coincide with the May and summer holidays, respectively. The spike just before the summer holidays is also notable, suggesting that many denial-of-service attacks are carried out by students.

Attacks can be carried out without major expense

The rise of DdoS as a Service (also known as booter or stresser services) is making it increasingly simple to carry out this kind of attack at low cost. It requires very little knowledge, and a payment by credit card or bitcoin is all that is needed [33] [34].

Conclusion

Denial-of-service attacks are here to stay. However, they are relatively easy to control, despite the possibility for malicious parties to use cheap services that require little knowledge or skill to carry out an attack. It is, however, important to remain vigilant, and to make sure that mitigating measures are effective (and remain so).

7. VULNERABILITIES CONTINUE TO BE A PROBLEM

Vulnerabilities in operating systems and IoT devices

Each year, many software vulnerabilities are found in large operating systems (Windows, macOS and Linux). However, IoT devices also contain vulnerabilities. While holes in major operating systems are routinely patched, this is not the case with IoT devices. Moreover, IoT devices contain many configuration errors that are difficult, or even impossible, for the user to repair. Because there are so many IoT devices, exploitation of a vulnerability of this kind can have major consequences. This was the case in late 2016, when the Mirai botnet took down Brian Krebs' website [35]. This botnet was also used in the DYN attack in October 2016, which led to a number of major internet services such as Paypal, Twitter, Spotify and Github being rendered inaccessible [36].

The illustrations below indicate which regions experienced problems due to the Dyn attack. It is clear that the second attack in the US was much more aggressive. This was measured on the network of Level3, one of the world's largest internet providers.

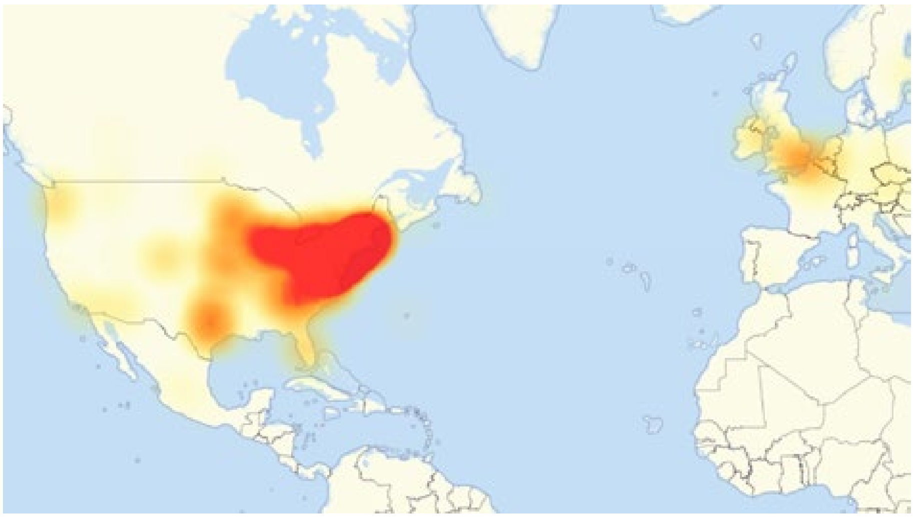


Figure 8: Internet problems on the morning of 21 October 2016 as a result of the first DDoS attack on Dyn (source: Threatpost)

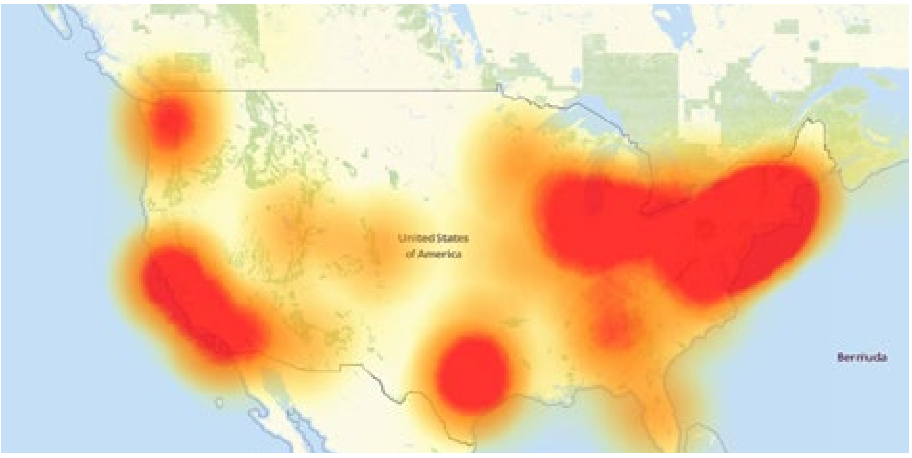


Figure 9: Internet problems on the evening of 21 October 2016 as a result of the second DDos attack on Dyn (source: Threatpost)

Zero-day vulnerabilities

Traditionally, criminals and state actors try to use unknown and, as yet, unpatched vulnerabilities – called zero-day vulnerabilities – to penetrate systems [9].

One example is the EternalBlue exploit, which was used in the Wannacry ransomware attack of May 2017 and later on in the NotPetya attack. The EternalBlue exploit is said to have been developed by the NSA [37].

According to Symantec, there was a slight fall in the number of zero-day vulnerabilities in 2016, possibly as a result of responsible disclosure programmes and improved software development. Symantec assumes that this has made zero-day vulnerabilities more difficult for malicious parties to find, and that they have therefore started using other simpler ways of carrying out attacks [16].

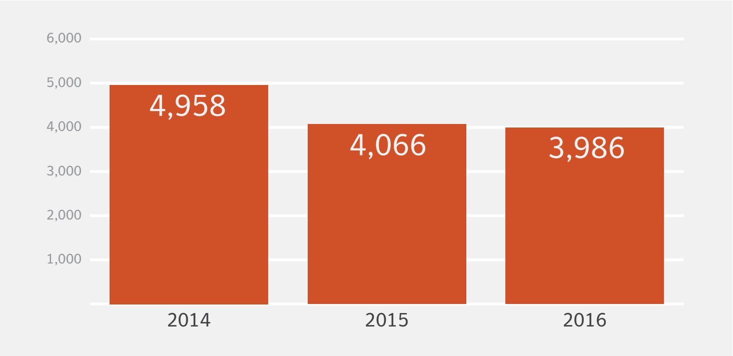


Figure 10: Number of zero-day vulnerabilities per year (source: Symantec – ISTR 22)

Vulnerabilities in mobile devices

A point of concern is the increase in the number of vulnerabilities in mobile devices, such as smartphones and tablets. Since students, teachers, researchers and other staff want, and are allowed to use these devices, it is a growing threat for education and research. Few smartphones and tablets are managed centrally; instead, they are a part of a BYOD policy (Bring Your Own Device). This constitutes a huge challenge for securing sensitive data effectively in student information systems such as Osiris and EduArte.

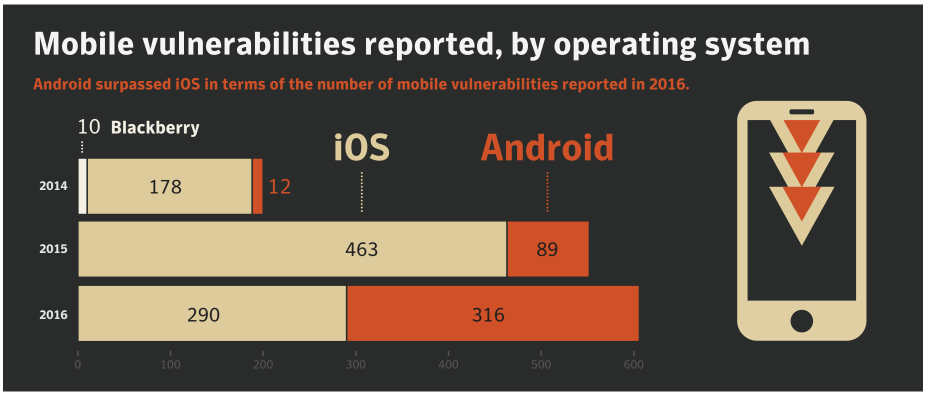


Figure 11: Increase in numbers of vulnerabilities in mobile operating systems (source: Symantec – ISTR 22)

Conclusion

Malicious parties continue to make frequent use of vulnerabilities in software despite the slight drop in the number of zero-day vulnerabilities. Although patches are still released for vulnerabilities, it is a case of too little, too late. This means that organisations are facing huge risks that they need to analyse carefully so that they may mitigate them effectively.

8. ATTACKERS

Varying motives and levels of skill

Actors with varying motives and levels of skill are responsible for carrying out attacks:

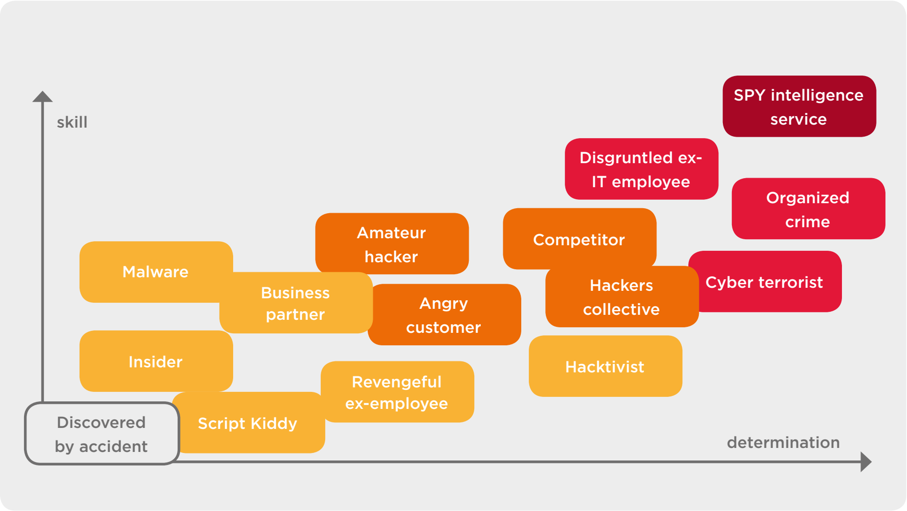


Figure 12: Skills and determination of actors

Six actors play a role in the education and research sectors. These are listed below in order of skills and motives from low to extremely high:

1. **Employees – skill:** low
   Employees benefit from good evaluations and performance; therefore, manipulating HR files may be of interest to them. Employees may feel resentment at the threat of dismissal or reorganisation and be incited to inflict damage. Some employees are potentially very skilled and have access to systems and networks. Other employees are often unaware of cyber security threats, which means they may be careless when handling sensitive information. In some cases, they are driven by efficiency and convenience rather than cyber security concerns.

2. **Students – skill:** low to medium
   Students benefit from good study progress, so it may be of interest to them to manipulate their grades. They already have access to many systems and networks, and some are very skilled. Many students are often unaware of cyber security threats, which means they may be careless when handling sensitive information.

3. **Activists and cyber vandals – skill:** low to medium
   Activists have decent knowledge and skills that they can use to steal data or make systems and networks inaccessible. Moreover, it is highly likely that they will make stolen data public. Cyber vandals are also looking for peer recognition, and sometimes want a large audience for their actions. Cyber-jihadists are intent on collecting sensitive data that they will make public for propaganda reasons subsequently.

4. **Competitors – skill: low to medium**
   Commercial parties benefit from obtaining information early from competitors. The same could be true for rival partner institutions which are interested in each other's research data, for example. Although knowledge and skills are available, they will not be used readily against a fellow institution.

5. **Cyber researchers – skill: high**
   Cyber researchers are in fact hackers, but have no malicious intent. If they encounter a problem, they will generally warn the institution concerned (responsible disclosure). They are extremely skilled, and do not always act in accordance with the institution's policies.

6. **Professional criminals and state actors – skill: high to very high**
   Professional criminals are driven mainly by financial gain. They sell stolen data or try to collect a ransom by making data temporarily inaccessible. They are organising themselves increasingly, making their chances of success much higher. A great deal of data is collected in the context of anti-terrorism and crime fighting, but commercial and economic motives (an interest in intellectual property and innovative knowledge) can also be an incentive for foreign intelligence agencies.

How actors affect threats

The image below shows the threats (see table 1, page 5) on which the various actors have an effect:

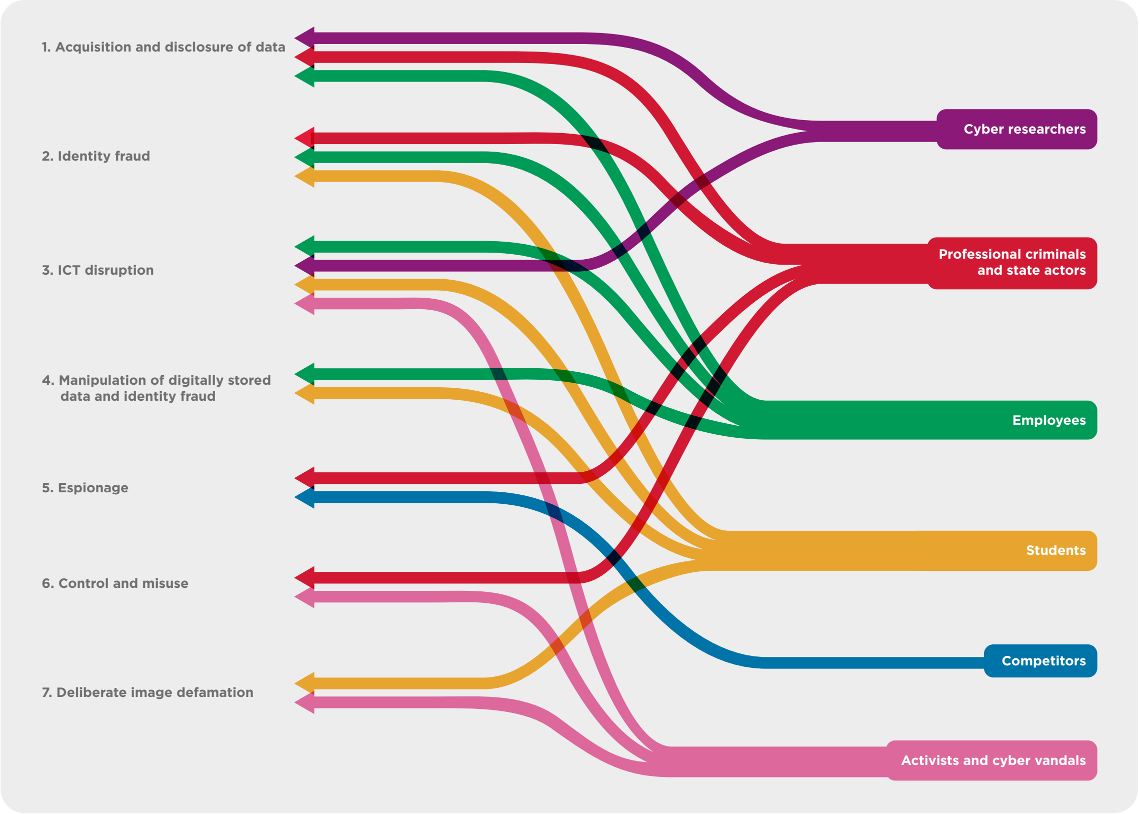

1. Acquisition and disclosure of data
2. Identity fraud
3. ICT disruption
4. Manipulation of digitally stored data and identity fraud
5. Espionage
6. Control and misuse
7. Deliberate image defamation
Cyber researchers
Professional criminals and state actors
Employees
Students
Competitors
Activists and cyber vandals

Figure 13: How actors affect threats

Conclusion

There are many different types of attackers, ranging from script kiddies to professional criminals and state actors. While harmless attacks by, for example, script kiddies, are simply annoying, attacks by professional criminals can cause major damage. Since the advanced attacks carried out by professional criminals and state actors are particularly difficult to detect, organisations need to mobilise advanced resources to defend themselves against those.

SOURCES

[1] 26 NCSC *Cybersecuritybeeld Nederland*, 21 06 2017 [Online] Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html [Opened 29 09 2017]

[2] VSNU, *VSNU Publicaties*, 5 September 2016 [Online] Available: http://www.vsnu.nl/files/documenten/Publicaties/VSNU_De_Digitale_Samenleving.pdf [Opened 29 09 2017]

[3] B. Bosma, SURF | *Cybedreigingsbeeld 2016 - SURFnet*, 17 11 2016 [Online] Available: https://www.surf.nl/kennisbank/2016/cyberdreigingsbeeld-2016.html [Opened 27 10 2017]

[4] AIVD, *Bent u zich bewust van de risico's van cyberspionage?*, 22 05 2017 [Online] Available: https://www.aivd.nl/actueel/nieuws/2017/05/22/bent-u-zich-bewust-van-de-risicos-van-cyberspionage [Opened 10 08 2017]

[5] SURF, *SURFnet Community of Incident Response Teams (SCIRT),* [Online] Available: https://www.surf.nl/diensten-en-producten/scirt/index.html [Opened 29 09 2017].

[6] Microsoft, *TN New ransomware, old techniques: Petya adds worm capabilities*, 27 06 2017 [Online] Available: https://blogs.technet.microsoft.com/ mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/ [Opened 29 09 2017]

[7] AIVD, *Jaarverslag 2016: dreiging voor Nederland onverminderd hoog,* 04 04 2017. [Online] Available: https://www.aivd.nl/actueel/nieuws/2017/04/04/jaarverslag-2016-dreiging-voor-nederland-onverminderd-hoog [Opened 29 09 2017]

[8] AIVD, *Jaarverslag AIVD 2015*, 21 04 2016. [Online] Available: https://www.aivd.nl/publicaties/jaarverslagen/2016/04/21/jaarverslag-aivd-2015 [Opened 29 09 2017].

[9] The Guardian, *The Snowden Files*, 02 12 2013 [Online] Available: https://www.theguardian.com/world/2013/dec/02/nsa-files-spying-allies-enemies-five-eyes-g8 [Opened 29 09 2017]

[10] AIVD, *Speech Rob Bertholee symposium iBestuur 'Grip op cybersecurity'*, 22 05 2017. [Online] Available: https://www.aivd.nl/publicaties/toespraken/2017/05/22/speech-rob-bertholee-symposium-ibestuur-grip-op-cybersecurity [Opened 29 09 2017]

[11] Statista, *IoT: number of connected devices worldwide* 2012-2025, 11 10 2017 [Online] Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ [Opened 11 10 2017]

[12] Juniper, *IoT Connected Devices to Triple to Over 38Bn Units*, 28 07 2017 [Online] Available: https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020 [Opened 11 10 2017]

[13] NRC-Handelsblad, *D66 wil keurmerk voor beveiliging IoT-apparaten*, 20 11 2016 [Online] Available: https://www.nrc.nl/nieuws/2016/11/20/d66-wil-keurmerk-voor-beveiliging-iot-apparaten-a1532668 [Opened 29 09 2017]

[14] Domotica.nl, *Chipgiganten sporen EU aan om Internet of Things-keurmerk in te voeren*, 07 06 2017 [Online] Available: https://domotica.nl/2017/06/07/chipgiganten-richtlijnen-iot/ [Opened 29 09 2017]

[15] NEN, *NEN richt normcommissie Internet of Things ('IoT')* op, 03 10 2017 [Online] Available: https://www.nen.nl/NEN-Shop/ICTnieuwsberichten/NEN-richt-normcommissie-Internet-of-Things-IoT-op.htm [Opened 10 10 2017]

[16] Symantec, *Internet Security Threat Report*, 04 2017 [Online] Available: https://www.symantec.com/security-center/threat-report [Opened 24 10 2017]

[17] Tweakers, *Ook Q-park krijgt te maken met aanval van ransomware*, 14 05 2017. [Online] Available: https://tweakers.net/nieuws/124649/ook-q-park-krijgt-te-maken-met-aanval-van-ransomware.html [Opened 27 10 2017]

[18] Deloitte, *Cyber Value at Risk in The Netherlands 2017*, 25 09 2017 [Online] Available: https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-value-at-risk-in-the-netherlands-2017.html [Opened 29 09 2017]

[19] Tweakers, *Aanval met NotPetya-malware kost Maersk tot 256 miljoen euro*, 16 08 2017. [Online] Available: https://tweakers.net/nieuws/128411/aanval-met-not- petya-malware-kost-maersk-tot-256-miljoen-euro.html [Opened 27 10 2017]

[20] Tweakers, *Minstens vier ziekenhuizen in Verenigd Koninkrijk getroffen door malware*, 14 01 2017 [Online] Available: https://tweakers.net/nieuws/120059/minstens-vier-ziekenhuizen-in-verenigd-koninkrijk-getroffen-door-malware.html [Opened 27 10 2017]

[21] CSR, *CSR Advies, 06 2017* [Online] Available: https://www.cybersecurityraad.nl/binaries/CSR-advies%202017%20nr.%202%20-%20Naar%20een%20landelijk%20dekkend%20stelsel%20van%20informatieknooppunten_tcm56-269317.pdf [Opened 29 09 2017]

[22] WRR, *Veiligheid in een wereld van verbindingen*, 10 05 2017 [Online] Available: https://www.wrr.nl/publicaties/rapporten/2017/05/10/veiligheid-in-een-wereld-van-verbindingen [Opened 29 09 2017]

[23] Rijksoverheid, *Kamerbrief over oprichting Digital Trust Centre*, 23 09 2017 [Online] Available: https://www.rijksoverheid.nl/documenten/kamerstukken/2017/09/23/kamerbrief-oprichting-van-een-digital-trust-centre [Opened 29 09 2017].

[24] NCSC, *Nationaal Detectie Netwerk | NCSC*, [Online] Available: https://www.ncsc.nl/samenwerking/nationaal-detectie-netwerk.html [Opened 24 09 2017]

[25] SURF, *SCIPR - community voor informatiebeveiligers en privacy officers*, [Online] Available: https://www.surf.nl/diensten-en-producten/scipr/index.html [Opened 29 09 2017]

[26] SURF, *SURFcert,* [Online] Available: https://www.surf.nl/diensten-en-producten/surfcert/index.html [Opened 24 09 2017]

[27] SURFaudit, *SURFaudit*, [Online] Available: https://www.surf.nl/diensten-en-producten/surfaudit/index.html [Opened 24 09 2017]

[28] SURF, *Cyber Save Yourself*, [Online] Available: https://www.cybersaveyourself.nl/ [Opened 24 09 2017]

[29] B. Bosma, *Rapport Resultaten SURFaudit benchmark 2015*, SURF, 09 06 2016 [Online] Available: https://www.surf.nl/kennisbank/2016/resultaten-surfaudit-benchmark-2015.html [Opened 24 09 2017]

[30] TNO, *TrustTester: veilig valideren van persoonlijke gegevens, 2016* [Online] Available: https://www.tno.nl/nl/aandachtsgebieden/industrie/networked-information/information-creation-van-data-naar-informatie/trusttester-veilig-valideren-van-persoonlijke-gegevens/ [Opened 29 09 2017]

[31] Stichting Privacy by Design, *Privacy by Design Foundation, 2016* [Online] Available: https://privacybydesign.foundation/ [Opened 29 09 2017]

[32] Overheid.nl, *Boetebeleidsregels Autoriteit Persoonsgegevens 2016*, 2016 [Online] Available: http://wetten.overheid.nl/BWBR0037543/2016-01-16 [Opened 29 09 2017]

[33] A. Orlowski, *Meet DDoSaaS, The Register*, 12 09 2016 [Online] Available: https://www.theregister.co.uk/2016/09/12/denial_of_service_as_a_service/ [Opened 27 10 2017]

[34] D. Smith, *The Growth of DDoS-as-a-Service: Stresser Services*, Radware, 18 09 2017. [Online] Available: https://blog.radware.com/security/2017/09/growth-of-ddos-as-a-service-stresser-services/ [Opened 27 10 2017]

[35] C. Osborne, *Krebs on Security booted off Akamai network after DDoS attack proves pricey*, ZDNET, 23 09 2016 [Online] Available: http://www.zdnet.com/article/krebs-on-security-booted-off-akamai-network-after-ddos-attack-proves-pricey/ [Opened 24 10 2017]

[36] L. Franceschi-Bicchierai, *Blame the Internet of Things for Destroying the Internet Today*, Motherboard, 21 10 2016 [Online] Available: https://motherboard.vice.com/en_us/article/vv7xg9/blame-the-internet-of-things-for-destroying-the-internet-today [Opened 24 10 2017]

[37] B. Krebs, *Eternal Blue - Krebs on Security*, 17 06 2017 [Online] Available: https://krebsonsecurity.com/tag/eternal-blue/ [Opened 27 10 2017]

[38] *Verizon, 2017 Data Breach Investigations Report,* Verizon, 2017.

COLOFON

Author
Bart Bosma

Editors
Jan Michielsen

Design
Vrije Stijl, Utrecht

Photography
iStock

December 2017

SURF

+31 (0)88 787 30 00
www.surf.nl

INTEGRALE
VEILIGHEID
HOGER ONDERWIJS

SURF