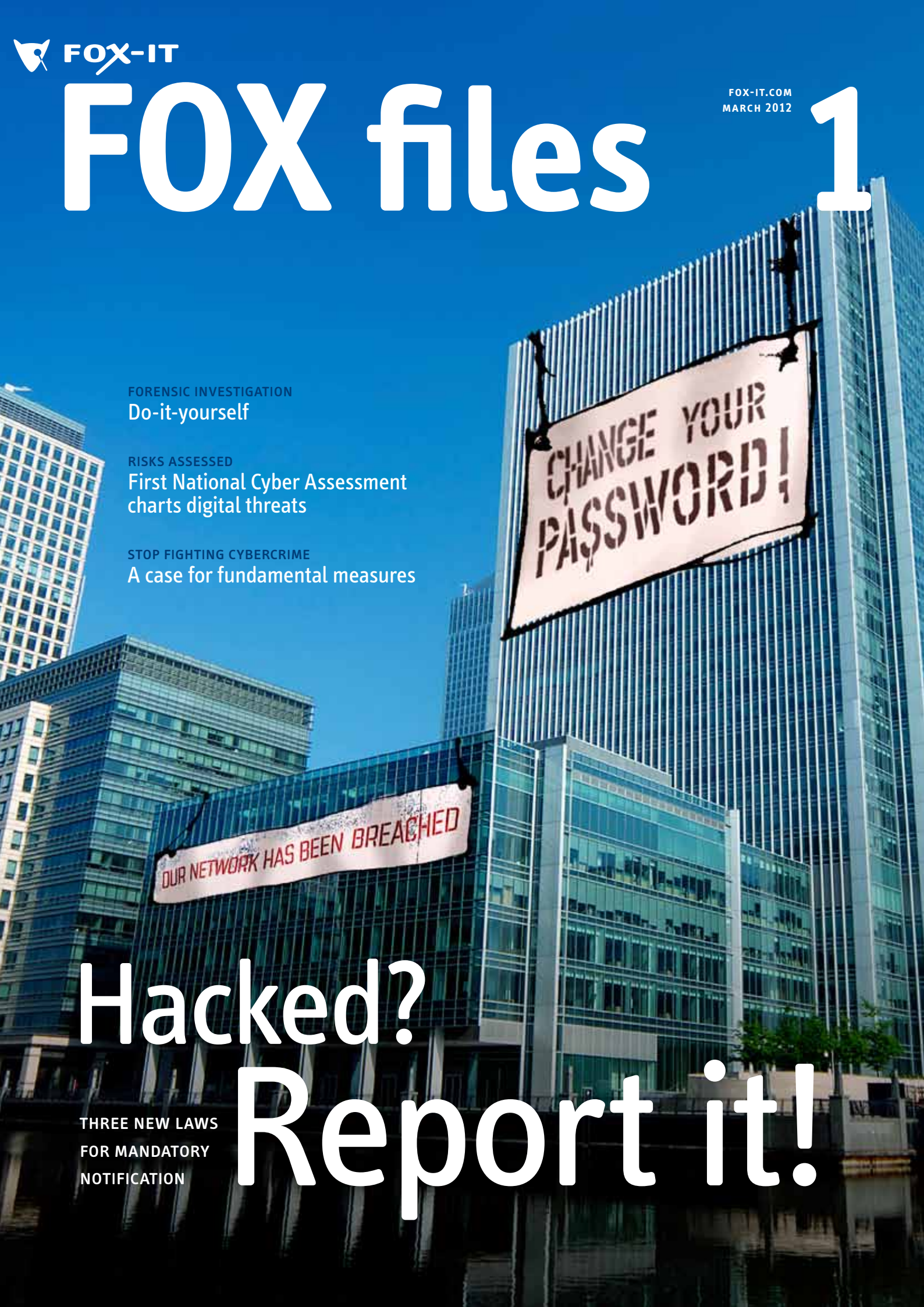
FOX-IT

FOX files 1

FOX-IT.COM
MARCH 2012



FORENSIC INVESTIGATION
Do-it-yourself

RISKS ASSESSED
First National Cyber Assessment charts digital threats

STOP FIGHTING CYBERCRIME
A case for fundamental measures

Hacked? Report it!

THREE NEW LAWS FOR MANDATORY NOTIFICATION

18

27

10

22

14

24

04

CURRENT AFFAIRS

04 Mandatory notification for data breaches

The media regularly report that organizations have been hacked. In response to recent serious data breaches, three notification obligation laws are now being prepared. The Dutch government particularly emphasizes (digital) data protection. It's important that organizations prepare themselves for this.

COLOPHON

Editorial address
Fox-IT Marketing Department
PO Box 638
2600 AP Delft
+ 31 (0)15 - 284 79 99
+ 31 (0)15 - 284 79 90
marketing@fox-it.com
www.fox-it.com

Design
viervier, Rijswijk

Photography
Chris Bonis, Rotterdam

Interviews and articles
Sabel Communicatie, The Hague

COLUMN

Cybercrime entrepreneurs

We believe the world needs to take advantage of the opportunities new IT technology offers. But this creates new cyberthreats we need to protect ourselves against. When Fox-IT started 13 years ago, protection could still be offered by a small group of people with the right expertise. In the meantime, an actual service industry has evolved in the underworld, driven by many 'bad' entrepreneurs. Cybercrime strikes at an enormous rate and scale, as borne out by recent incidents such as Google, KPN and Sony.

How different it looks among the adversaries. Governments are taking measures and cybersecurity centres are being opened everywhere. It remains uncertain as to whether the approach of these centres is effective enough in the increasingly rapidly evolving cyberdomain. Ironically enough the corporate world is lagging behind; the number of new IT security companies is negligible.
It's nice to have little competition, but within this growing problem field we would all be helped if there were a few more specialist players. The demand for cybersecurity is unprecedentedly high. Why is the entrepreneurship not blossoming? There has been enough time to find and employ the right people.
To take a serious stand against cyberthreats we need complex new knowledge and solutions. Innovation has traditionally been a solid but slow process of scientific research which is then applied commercially. Speed is certainly required, with the development of the criminal market progressing at such a rapid pace. And that's the crux of the matter.
In the current situation it's time to be pragmatic in the search for solutions. Operational knowledge, intelligence from the underworld and technical research are the ingredients for success. This requires a very special combination of clever people and collaboration between the corporate world, the government and educational institutions.
The formula for entering this market is a difficult, but not impossible. We would like to help newcomers by sharing our knowledge, so that we can work towards a more secure society together.

Menno van der Marel, Fox-IT CEO

CURRENT AFFAIRS

Mandatory notification for data breaches

MORE FOCUS ON PROTECTING PERSONAL DATA

Three new laws requiring notification are in the pipeline in the Netherlands, each dealing with protecting (personal) data. It's important that organisations prepare themselves for this. What do the proposed notification obligations entail, what measures can you take as a company to avoid a hack, and how do you communicate if you have been hacked?

‘The bill for the mandatory notification for ISPs still has some rough edges’

Organisations working with personal data should by now be aware that they must protect this sensitive information. But hackers are becoming increasingly more inventive and their attacks more advanced. So how do you know as an organisation just what constitutes adequate protection? And what should you do if you are nevertheless hacked and sensitive information has gone public? Apart from it being advisable that you communicate about this openly and clearly, you will shortly also be required to notify the breach. Four notification laws are planned, through which the legislator requires organisations to report the hack, on pain of the imposition of a fine. There are both advantages and disadvantages to these mandatory notifications.
Jan-Jaap Oerlemans, Fox-IT legal advisor and a PhD student at the eLaw@Leiden centre of Leiden University, explains the four different mandatory notifications.

EXISTING MANDATORY NOTIFICATIONS IN THE NETHERLANDS

‘The ICT mandatory notification is not entirely new in the Netherlands,’ explains Jan-Jaap Oerlemans. ‘There is already a mandatory notification for breaches of state secrets, a mandatory notification for exchange-listed companies to reveal price-sensitive information, and the possibility to arrange a mandatory notification contractually or to enforce it.’

MANDATORY DATA BREACH NOTIFICATION BILL FOR ISPS AND TELECOM COMPANIES

The Senate is considering a bill from the Ministry of Economic Affairs, Agriculture and Innovation for a mandatory notification for Internet Service Providers (ISPs) and telecom companies. The mandatory notification is divided into two reporting obligations: one if a hack has had consequences for the protection of personal data, and a second if a data leak puts the delivery of its services at risk. Discussions on this mandatory notification date right back to 2006; the expectation is that this bill will be approved within a few months. Jan-Jaap Oerlemans: ‘The bill for the mandatory notification for ISPs still has some rough edges. For example, a data leak with “unfavourable consequences for those involved” must be reported to the OPTA independent authority. It will determine whether those involved should be notified. However, for companies it is not yet clear precisely when a notification is required to be submitted. What are the “unfavourable consequences” for instance? More clarity is needed on this. Or better: ideally the OPTA should draw up policy rules to remove any lack of clarity.’

Should the mandatory notification be ignored, the OPTA can impose a fine of up to 450,000 euros. However, there are exceptions: if the authority believes that the provider “has taken suitable technical protection measures” (for example by encrypting the data), then notification of the data leak may be omitted. Jan Jaap Oerlemans: ‘But if the keys have been stolen, encryption has no point. It’s up to the OPTA to determine how great the risk is that the personal data will go public. Based on the outcome, the OPTA will then determine whether a company must notify the incident to those involved or whether the company is subjected to a fine.’

GENERAL MANDATORY DATA BREACH NOTIFICATION BILL

The general mandatory data breach notification bill has recently been put out “for consultation”. This means that the proposal has not yet been sent to the House of Representatives, but is in a preliminary phase in which experts can respond to the draft proposal. ‘The proposed mandatory notification applies to every organisation which is “responsible” in the sense of the Personal Data Protection Act (WBP in its Dutch acronym). The mandatory notification applies to both public and private parties, such as local authorities, hospitals, webshops and social network sites,’ explains Jan Jaap Oerlemans. ‘So this covers situations where there has been a breach of the security measures and there is a significant risk of the loss of confidentiality of personal data.’

‘The European Commission is also busy updating the general privacy guideline with a general mandatory notification. The commission needs more time to achieve European regulation, so the Dutch mandatory notification is being established in the interim. Ultimately this will change after a few years, once the European regulation applies.’

PROPOSED CHANGES TO DRAFT BILL

Jan Jaap Oerlemans: ‘Apparently the cabinet already wants to change the proposed mandatory notification. A general mandatory notification is proposed in the draft bill, which would apply to both public and private parties.’

FOUR TYPES OF MANDATORY NOTIFICATION

In the Netherlands four types of ICT mandatory notification can be distinguished, of which three are still a (draft) bill.

1. The existing mandatory notification for the protection of state secrets and price-sensitive information, among others.
2. The mandatory data breach notification bill is expected to be approved shortly by the Dutch Senate.
3. The general mandatory notification for any breach of security measures that imposes a risk to a loss of confidentiality of personal details has been assigned ‘for consultation’; this means experts may respond to the proposal. Introduction is expected to take up to two years.
4. The security breach notification bill will go to the Dutch House of Representatives by September 2012 at the earliest.

‘From the ICT business sector we would like to cooperate with the government’

‘Be transparent and describe what has happened’

CRISIS COMMUNICATION FOR DATA BREACHES

Revealing a data breach leads to reputational damage, so companies or bodies will initially attempt to avoid a situation that needs to be reported. But what if the security turns out not to be satisfactory, how do you then react? Bart Schermer, partner with ICT consultancy Considerati: ‘Even if you are well-prepared and your security is in order, an incident can always occur. Mandatory notification or not, it is always important that you do not keep the data breach under your hat. If it gets out, then you will be even worse off. So it’s better to own up immediately and to reveal all with an honest and well-substantiated account. Explain just what actions and measures you are taking. You are then honest, open and exhibit decisiveness.’

ASSESSING SECURITY LEVELS

Using an impact assessment companies or bodies can estimate the security level they need. Bart Schermer: ‘You obviously don’t want to spend ten cents protecting five. You arrange adequate protection of the data on the basis of the assessment. If things do go wrong, you can in any case show that you did your best to secure things well.’

HONEST AND TRANSPARENT

How does general crisis communication differ from the communication for data breaches? Bart Schermer: ‘The most significant difference is that for data breaches you need to explain more about the background and you need to give more advice on what those involved can do themselves.’
Once hacked, says Bart Schermer, there are six communication steps to be taken:

1. Be transparent and describe what has happened.
2. Explain what you have done to attempt avoiding being hacked.
3. Explain that things went wrong despite this security; be open about the kind of hack to which the security was not equal.
4. Offer apologies and explain that you are working on better security.
5. Describe in clear language the steps those involved could take themselves to limit any damage as far as possible; for example, advise them to change passwords, to keep an eye on bank account movements, or even to apply for a new credit card.
6. Show your clients that you consider them to be important, and offer those who are victims something extra, such as three months’ free membership or a free product.

‘Timing is crucial’, Bart Schermer emphasises. ‘Clients want to have control over their personal data. If as a company your notification and the steps to be taken are too late, then your well-intentioned communication and proposed measures will already be far less effective.’

What does the Dutch proposal entail? Hacked organisations that fall within the general mandatory notification must report this to the Dutch Data Protection Authority (CBP in its Dutch acronym). This authority will then determine whether those involved should be notified and may impose a fine of up to 200,000 euros on organisations. To avoid this, companies or bodies working with personal data must therefore protect themselves well. ‘This general mandatory notification is aimed purely at breaches of the security measures that have been implemented to protect personal data,’ explains Jan-Jaap Oerlemans. ‘This arises from the existing obligation to take security measures on the basis of Section 13 of the Personal Data Protection Act.’ Recently the CBP publicly sounded the alarm, because it lacks the manpower needed to perform these tasks.

MANDATORY SECURITY BREACH NOTIFICATION BILL

The mandatory security breach notification is a motion from VVD Member of Parliament Jeanine Hennis-Plasschaert following the DigiNotar affair. Jan-Jaap Oerlemans: ‘This mandatory notification concerns more than just the protection of personal data. It applies specifically to organisations with critical infrastructures such as hospitals, energy utilities or the tax and customs administration. Should such an organisation be hacked then this breach must be notified to the National Cyber Security Centre (NCSC). The centre may then take action.’ It’s not yet clear just how this bill will look; more clarity will most probably emerge before the 2012 summer recess.

CONFUSING

‘Shortly, we will have four types of mandatory notifications for data breaches running in parallel, and that’s problematic,’ Jan-Jaap Oerlemans concludes. ‘The divisions are not clear. For example, a multinational may find itself involved with all four mandatory notifications. Or an exchange-listed energy utility with three mandatory notifications (namely price-sensitive information, general mandatory notification and a mandatory security breach notification concerning critical infrastructure). Which body should such a company report the hack to? It’s therefore up to the legislator to take account of any possible overlaps.’

ADVANTAGES

Is the forest of mandatory notifications not a hindrance to the objective towards which the government is striving? ‘Four arguments can be advanced in favour of a mandatory notification,’ explains Jan-Jaap Oerlemans. ‘The most important is that clients are notified should there be a data breach and that they can therefore take their own measures to limit the damage. For example, they could change their password in good time, or could choose another company. Another advantage is that reputational damage or a considerable fine are stimulating companies to ensure adequate protection of the personal data. This leads to a third argument, namely the side effect that notifications immediately provide more clarity on the scale on which hacking personal data occurs, and that knowledge about hacks can help to prevent similar attacks against other organisations. The final argument is that consumer confidence in electronic service providers will rise, despite the notification of a hack, because the companies are more transparent and as a result clients get the impression that they have more control.’

‘You obviously don’t want to spend ten cents protecting five’

OBJECTIONS

But there are also counter-arguments. Bart Pegge, policy advisor for the sectoral organisation ICT-Office: ‘We lack a good definition. What, for example, is a “serious” incident? Here you need to look at the scope (how many people were involved in it?) and the type of data (have only names and addresses gone public, or also birthdates and bank account numbers?). From the ICT business sector, we would like to cooperate with the government in achieving a good bill. We also think that imposing a fine is the wrong measure: by thinking in terms of sanctions you throw up barriers so that organisations are more inclined not to report an incident. It would in fact be better to actually reward a notification, so that an organisation is invited to be transparent. We also believe that the regulator should have a supporting role rather than a sanctioning one.’ Bart Pegge also thinks the timing of the bills is unfortunate. ‘Wait until the new privacy law has been completed in Europe and then link the Dutch mandatory notification to it. That will still take two years, but it avoids duplicating work and any confusion about reviewing the rules.’

QUICK QUENCHING

Bart Pegge is more critical of the security breach notification. ‘We are against it. A notification should be focused on containing the effects of the incident as quickly as possible. For critical infrastructures you don’t want any administrative rigmarole, rather you want to open the door wide for the fire brigade. You need some quick quenching! So rather focus on crisis response and support. Obligations and forms only ensure that organisations prefer to cover up their incidents.’ ■

Hunt for the modern Jesse James

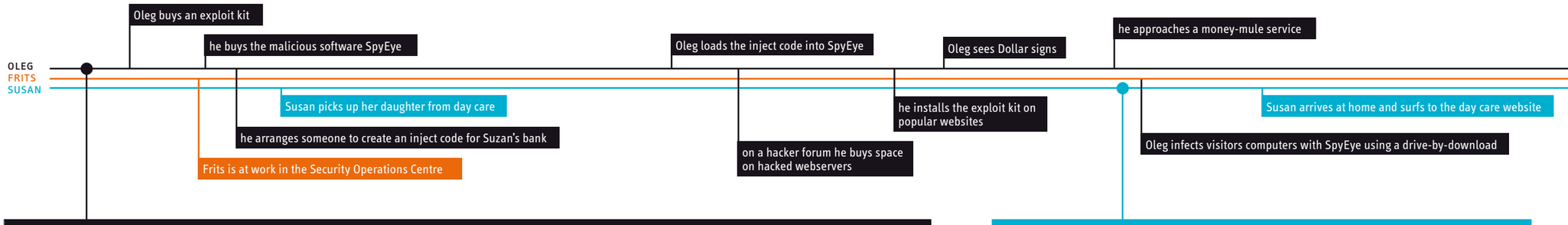
FRAUDULENT ONLINE TRANSACTION SPOTTED ON TIME

OLEG is 22 years old and lives in St. Petersburg. He's had a good education, but unemployed.

SUSAN is account manager and lives 2,000 kilometres away in a pleasant semi-detached home in Utrecht.

FRITS works at the Security Operations Centre (SOC).

The modern bank robber doesn't have a horse, a cowboy hat and saddlebags, but operates in front of his computer in an attic. Thanks to cunningly injected malware they steal millions of euros from bank accounts in the Netherlands alone, without the victims being directly aware of it. With the DetACT managed security programme the Dutch banks and Fox-IT have launched the hunt for these online bandits. What follows is a reconstruction of how Susan was almost robbed by Oleg.



Since his eighteenth birthday Oleg has been earning his money through cybercrime, and specialises in digital bank robbery. He's an experienced cybercriminal who knows exactly what he has to do and where he has to be. At the start of his career he avoided the Netherlands, because digital fraud in other European countries was easier. But now the situation has changed: the security of online banking has been tightened everywhere, and he now has access to better tools than in the beginning.

PREPARATION IN RUSSIA

Oleg invests a lot of money in intermediaries and extensive software. Shortly he wants to inject transactions, hiding these transactions in his victims' credits and debits overview, and blocking the downloading of statements so that his victims remain unaware.

This is why he buys the Blackhole exploit kit. An exploit kit uses the vulnerabilities in software in computers. Unsuspecting internet users are led to this exploit kit through an infected website so that they can be infected with yet more malware.

Oleg also buys the malicious software SpyEye. This malware specialises in changing internet pages – which is precisely what Oleg intends to do. He then arranges that someone will produce a so-called inject code for the bank Oleg has an eye on. This code, which he loads into SpyEye, contains the formula for the changes Oleg intends: he wants to secretly add transactions in the online banking session, which first lead to so-called money mules, and then to himself. All this without the victim being aware of anything.

On a hacker forum he also buys space on hacked webservers in order to install his exploit kit on a number of frequently-visited websites. Using a drive-by-download, where a computer becomes infected immediately a website is opened, he places SpyEye on visitor computers.

'To be able to break into online bank transactions, Oleg invests a lot of money in intermediaries and extensive software'

Finally, Oleg approaches a money mule service which recruits Dutch bank account holders to operate as launderers. The launderers receive a percentage and deposit money in Oleg's digital wallet.

MEANWHILE IN THE NETHERLANDS

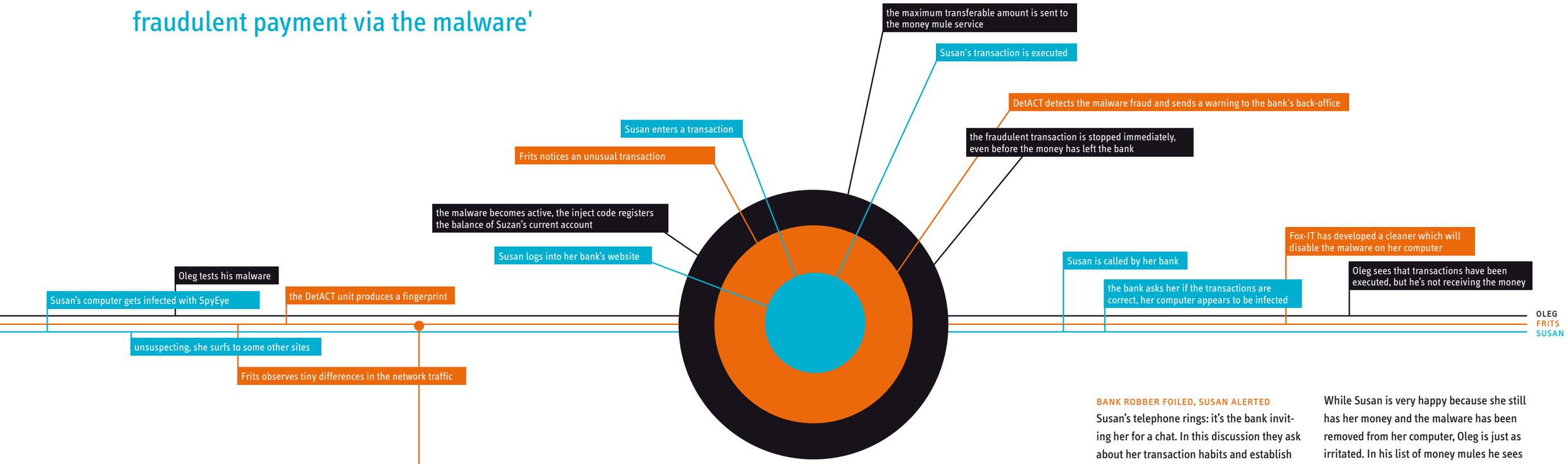
Susan is at her computer and accesses the site of her daughter's day-care centre. The service provider employed by Oleg has infected this website. Susan's computer is immediately infected with SpyEye. Susan then surfs to a number of other sites; she uses her computer in her normal way while in the background, the malware is waiting to strike. Susan is totally unaware of any of this, and her virus scanner has also not detected anything. Then Susan logs into her bank's website...

THE MALWARE STRIKES

Fortunately Susan's bank uses Fox-IT's service, DetACT for Online Banking. Frits is in the Security Operations Centre (SOC) office keeping an eye on banking traffic. He monitors all DetACT installations. As soon as Susan logs in, the malware kicks into action. The DetACT server observes Susan logging in and notices an unusual transaction. Specifically, a payment takes place immediately after logging in, where normally there would be a greater time delay.

Once Susan has logged in, the inject code records the balance of her current account and sends the maximum transferable amount to the money mule service, which then selects a suitable money mule. Susan wants to pay an invoice and enters the transfer. The inject code then asks her to enter her authorisation code, which she does; after all, the address field does show the bank's correct URL. Now two transactions are executed: the amount that Susan transferred and the false payment via the malware. Susan does not see this last, injected transaction: her balance is even adjusted by the malware so that it looks to Susan as though nothing out of the ordinary has happened.

'Two transactions are carried out: the amount Susan transferred and the fraudulent payment via the malware'



DETACT IN ACTION

Fox-IT's Intelligence department has already produced a detection engine for this attack, since before he launched his attack for real, Oleg tried out the malware on a limited scale. Thanks to their detective work Fox-IT's intelligence guys had gotten hold of the malware and unravelled it (reverse engineering) and identified the inject code. Oleg's test malware in fact exhibited tiny differences in the network traffic – actions which occurred a little differently to those a normal client would carry out. The DetACT unit produced a recognition pattern of this (a fingerprint), which could then be detected in other instances.

Back to Susan's transaction. Her bank's webserver regards the fraudulent transfer as a valid transaction and forwards it to the bank's back-office. At the same moment, DetACT detects the malware fraud and sends a warning to this back-office. The fraudulent transaction is immediately blocked, even before the money has left the bank. Oleg's malware 'thinks' that the money has been stolen and transferred, but the money mule receives nothing.

'DetACT detects the fraud and sends a warning to the bank's back-office'

BANK ROBBER FOILED, SUSAN ALERTED

Susan's telephone rings: it's the bank inviting her for a chat. In this discussion they ask about her transaction habits and establish that her computer has been infected. They notify her of a cleaner which Fox-IT has developed specially for her bank and which will disable the malware on her computer. Susan also learns the best way of working with her computer and online banking in the future.

While Susan is very happy because she still has her money and the malware has been removed from her computer, Oleg is just as irritated. In his list of money mules he sees that the transactions have been executed, but he's not receiving the money. He had expected his original investment to be repaid fifty times over, but DetACT has thrown a spanner in the works. Should Oleg decide to try again, he will probably choose a different bank, perhaps even in a different country. ■

The names in this reconstruction are fictitious, but the situation sketch is realistic. This is in fact just one of the possible attack scenarios.

FOX DETACT FOR ONLINE BANKING

How safe is online banking? Banks protect their online banking traffic with systems in bunkers, plenty of firewalls, encrypted HTTPS connections, authorisation codes and other measures. But cybercriminals have adapted their methods to all this. With phishing and malware they focus on the unsuspecting consumer whose PC, laptop, iPad or smartphone is difficult to protect.
In online banking the TCP/IP communication contains a wealth of data. Fox DetACT for Online Banking analyses this data. The system keeps an eye on all the bank's transactions non-stop, searching for divergences that (might) indicate fraud. Once DetACT detects a fraudulent transaction, the system sends a notification to the back-office of the bank. The bank then immediately goes into action to block fraudulent transactions. For more information see www.foxdetact.com.

First National Cyber Assessment charts digital threats

Opening NCSC by Minister Ivo Opstelten

CURRENT AFFAIRS

The government is working on an integrated approach to cyber security. What digital threats actually exist? And what are the most significant objectives of cybercriminals? The first Netherlands National Cyber Assessment (CSBN in Dutch) provides answers to these questions.

DISTINGUISH

NCSS: National Cyber Security Strategy. With the NCSS the cabinet gives shape to the integrated approach to combat cybercrime announced in the coalition agreement.

NCSC: National Cyber Security Centre. The NCSC was established at the government's initiative and will contribute to increasing the defensibility of Dutch society in the digital domain, and thus to a safe, open and stable information society.

CSBN: Netherlands Cyber Security Assessment. The CSBN provides an insight into the problems of cyber-security and draws an underlying distinction between various types of threats in the cybersecurity field.

The CSBN was issued in December 2011 and links to the National Cyber Security Strategy (NCSS) issued by the cabinet earlier that year. One of the action points in this strategy is producing adequate and up-to-date threat and risk analyses, to strengthen the Netherlands' defensibility. The first National Cyber Assessment was drawn up by Govcert.nl, which was merged as of 12 January 2012 into the new National Cyber Security Centre (NCSC). In developing the cyber assessment Govcert.nl focused on the threats in the ICT domain for the Dutch situation, while also taking account of developments abroad. At the end of last year, the threat analysis was presented to the Dutch House of Representatives by Minister Opstelten of Security & Justice. It is intended that an updated version of the National Cyber Assessment will be produced twice a year.

FIRST IDENTIFY RISKS, THEN THE APPROACH

Erik de Jong of Govcert.nl was responsible for developing the CSBN. He led the project and was the lead author of the eventual report. Starting from 1 April, he will be working for Fox-IT as a senior cybercrime expert. 'Understanding the risks is vitally important for cybersecurity. What do we need to protect ourselves against? What do we need to invest in? Only once the risks have been clearly charted we can develop a concrete approach.' Many parties were involved in developing the Cyber Assessment.

'To fight cybercrime you need to understand the risks'

From the government, such as the AIVD and KLPD, but also from the private sector such as KPN. 'Companies can provide important input on threats they identify in practice,' explains Erik de Jong.

DELIBERATE THREATS

The emphasis in the first CSBN is on deliberate threats rather than those arising from human failings. The Cyber Assessment shows that digital espionage and digital crime are the most important threats currently confronting the Netherlands. In 2011, both government and private organisations were the target of digital espionage. These cyberattacks were focused on obtaining confidential economic or political information. An example of this is the attacks on DigiNotar and the spread of the Duqu virus.

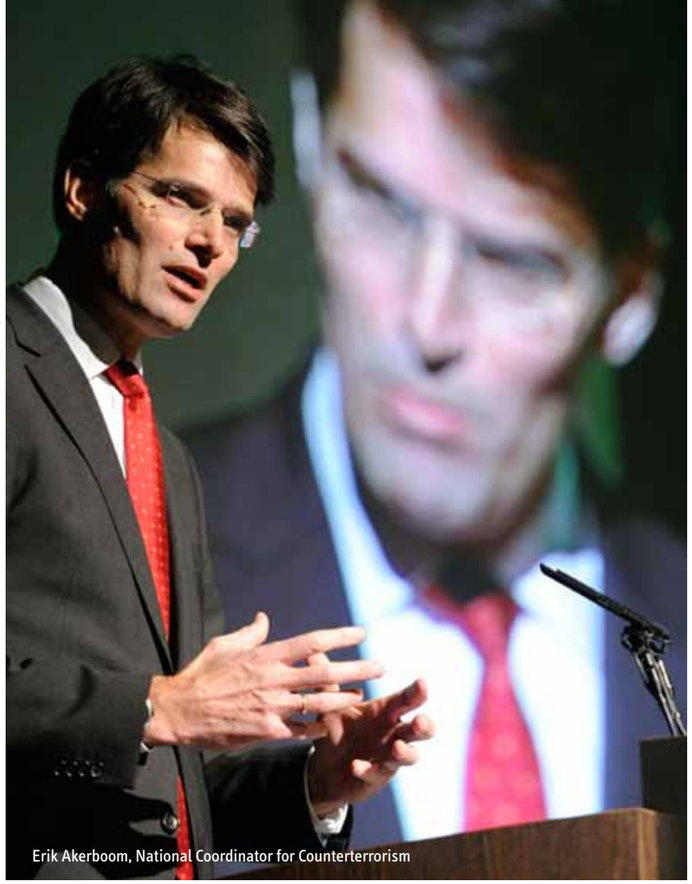
Although digital espionage is a growing threat, most attacks still fall under digital crime. This form is also the most apparent for society. Both the government and the corporate world, as well as citizens, can be the victim of digital crime. De Jong: 'We should not underestimate these threats. Attacks are becoming increasingly advanced and more complex. And it will happen to an increasing degree that a normal citizen in the Netherlands experiences the conse-

CYBER ASSESSMENT IS A WORK IN PROGRESS

At the presentation of the National Cyber Security Strategy (NCSS) in June 2011 the House of Representative argued for more clarity on the nature and scope of the problems the strategy was designed to tackle. We asked two members of parliament for their opinions.

Sharon Gesthuizen (SP): 'I believe that the importance of a secure ICT environment has been underestimated for too long. Only after the DigiNotar affair was the cabinet open to an integrated vision of cybersecurity. But in order to develop such a vision, the cabinet first has to list the requirements and the expectations of the private sector. In terms of the first Cyber Assessment the intentions are absolutely good. The cabinet is working on a realistic assessment of the problems and the threats. Now the task is to achieve the transition, where the connection between security and privacy may not be lost sight of.'

Gerard Schouw (D66): 'I regard the Cyber Assessment as an initial description. It is still not very specific, and the NCSC really needs to substantiate the results better. What is really going on? Are the threats really so terrible? I want to see statistics: how often is a bank actually hacked? Based on this report I still cannot evaluate just how serious the threats are. This National Cyber Assessment has certainly taken its first interesting steps. But when the second Cyber Assessment appears in June, it really needs to be a lot more concrete than the first attempt.'



Erik Akerboom, National Coordinator for Counterterrorism

'Everyone can experience the consequences of a cyberattack'

quences of a cyberattack.' Alongside the most significant threats, the CSBN discusses the various players, vulnerabilities and the tools the players deploy, such as exploits, malware and botnets.
How can the CSBN prevent governments, companies and citizens falling victim to a cyberattack? 'The National Cyber Assessment does not answer this question,' says Erik de Jong. 'We only describe the way the world looks. Nor does the Cyber Assessment describe any generic measures to combat cybercrime. It is purely a basis from which to develop an integral approach.'

NCSC: CENTRAL COMMUNICATION POINT

Now that Govcert.nl has merged into the new NCSC, this centre is working further on the threat analysis. This also fits in perfectly with the NCSC's mission: contributing to enhancing the defensibility of Dutch society in the digital domain, and - in doing so - to a safe, open and stable information society. From now on the NCSC will be the single communications point for cybersecurity, and should grow to become the expertise centre in the cybersecurity field. To this end the NCSC distributes information and supports organisations in adopting measures.
As the Manager of the Cyber Security directorate of the National Coordinator for Counterterrorism and Security (NCTV), Wil van Gemert is responsible for the further shaping of the NCSC. 'The NCSC gets a number of duties,' explains Wil van Gemert. 'An important task is incident response, handling ICT security incidents, in which the NCSC coordinates the response to ICT incidents where national security is at risk. Another important task is knowledge sharing, such as with the publication of the CSBN. But we also publish white papers, for example on cloud computing, and every day we publish current warnings on our website. The NCSC also plays a vital role in crisis coordination. To this end, in 2012 we will be working on the further development of the ICT Response Board. This is a joint public-private collaboration which meets if an ICT crisis threatens or occurs.' As already mentioned, the NCSC also works on expanding the CSBN. Because as Wil van Gemert notes, the first National Cyber Assessment is an excellent first step, but needs to be worked out and augmented still further. ' It is a work in progress. We still need to have an even better map of just where we are most vulnerable, so that we can set the right priorities.' To substantiate the CSBN better in qualitative terms, the number of partners providing input will be extended. In this way the NCSC will get even better information about concrete threats. It will also work on a better figure-based substantiation of the analysis.

'The commitment of companies and institutions is vitally important'

COLLABORATION IS CENTRAL

Collaboration between public and private parties is central in the NCSC. Wil van Gemert: 'We already have a few permanent partners, but I would like to extend this number still further. We want to make the cyberenvironment safer, and the commitment of companies and institutions is vitally important for this. They themselves are responsible for their own cybersecurity. We are not a regulator, but we make knowledge and expertise available and help organisations to take the right measures.' ■

INTERESTING WEBSITES

- www.rijksoverheid.nl/cybercrime
- www.ncsc.nl

SUMMARY OF THREATS PER GROUP AND OBJECTIVE

THREAT GROUPS \ OBJECTIVES	Government	Private Organisations	Citizens
States	Digital espionage and sabotage	Digital espionage and sabotage	
Private Organisations		Digital espionage	
Hacktivists	Publication of confidential data and digital disruption	Publication of confidential data and digital disruption	Publication of confidential data
Terrorists	Sabotage	Sabotage	
Professional criminals	Cybercrime (including digital [identity] fraud). Side effect: disruption by malware infection	Cybercrime (including digital [identity] fraud). Side effect: disruption by malware infection	Cybercrime (including digital [identity] fraud)
Scriptkiddies	Digital disruption	Digital disruption	

Threat level
high
moderate
low

OPINION

‘Let’s stop fighting cybercrime’

Cybercrime has been combatted for some time and this appears to be successful. But is this really so? Fox-IT CEO Ronald Prins on standards, security levels and responsibility.

In mathematics, but also in the ‘real’ world, we work with standards. In traffic the law regulates standards important for a safe society, like speed limits. If I was driving too fast according to the speed cameras, I am hit with a fine, even though I was maintaining a safe speed according to my own standards. Everyone maintains individual standards, but the yardstick is the standards which have been agreed by society.

SETTING STANDARDS

In cyberspace setting standards is not easy. There’s no-one with a laser gun and the maximum speed is also not known. This is virgin territory for both users and law enforcement. Once we have set standards, it’s time to start fighting cybercrime again.

SUCCESSES

Bredolab was a botnet of 30 million infected computers, used to plunder bank accounts and send out spam. This botnet was brought down last year and the Armenian suspect was apprehended. This suspect’s income was easily a million US dollars a month. Another example. In November the Dutch Banking Association (NVB) revealed that cybercrime-related fraud had doubled within a year. Every day Fox-IT protects a number of Dutch banks against fraud during online banking. Each month more fraud is stopped than the month before. Both camps – the criminals and the enforcers – celebrate their successes.

TIME TO MARK TIME

The successes above give us the impression that we are doing well in fighting cybercrime. But we must not forget that the opponents are also making great strides. Cyberspace is a dream place for criminals: breaking in is easy and there’s not a huge chance of being caught. That’s why it’s time to mark time and to give serious thought to the next step.

VULNERABLE WEBSITES

ICT journalist Brenno de Winter showed with Lektober (a pun on Leaky October) how simple it is to find a data leak. Since then vulnerabilities have been published almost daily, often in well-known websites. We later investigated some of the sites that had been hit. It is clear that there was something technically amiss with these sites; often even basic precautions were lacking.

Perhaps more alarming is the attitude of the organisations that were hit. Often they had already been subjected to an extensive audit. Respectable companies checked all the agreed issues, such as the password policy. These companies regularly missed the most basic things like default accounts and passwords for system administrators. Fortunately, some audits were of sufficient quality, but the recommendations were then not implemented. The reasons given for this were costs that were too high, an incomprehensible report or a restored backup which reversed the measures.

> ‘In the real world the police carry weapons, but in cyberspace everyone is equal’

RAISING SECURITY LEVELS: IT’S POSSIBLE

How do we resolve this security problem? A well-rehearsed argument is that there’s no such thing as 100% security. That’s true, but 95% is perhaps possible. The security level of some of the Lektober sites was far below the threshold, say 10%. Here there is much to gain.

A number of obvious ways to jack up security levels are:

1. Security by design You can’t ‘add’ security later on, you need to design it in right from the start.
2. Knowledge Knowledge of security is not yet adequate everywhere. Analysis of the Lektober incidents shows that programmers often forgot basic elements such as input validation. It only takes five minutes to explain, so why is it not done?
3. Focus Security and business continuity are often at loggerheads with each other. So it’s not useful to combine these two tasks in one person.

4. Balance Don't only concentrate on preventive measures but also implement 'detective' measures. It's probably not possible to make systems 100% watertight, but you can certainly detect whether a hacker is present. Invest in Intrusion Detection systems or subscribe to a managed service for this.

'An annual audit does not protect against real security risks'

THREE REASONS WHY IT DOESN'T HAPPEN

The list above is not new and any security expert could produce or improve it. The real question is why it doesn't happen. Three possible reasons:

1. Awareness Perhaps the DigiNotar case opened eyes. Ministers had to stay up nights because of a hacked company. Since then cybersecurity has been a regular topic of discussion in parliament.
2. Money If we had been more aware of the dangers, perhaps we would have spent more money on them. In times of economic crisis and short-term incentives like bonuses, people are quick to economise on security.
3. Security is not the same as compliance Many organisations put their trust in hallmarks, audits or other forms of compliance. An annual audit does not protect against real security risks; often they have little to do with each other and can impart a false sense of security. In short, the audit has the effect of letting real security deteriorate. The solution for the causes just mentioned is that the government assumes the initiative. There is no time to wait until 'those in charge' see the light. The examples mentioned represent cybercrime and direct financial losses. In the current society, where everything is interlinked, there are major concerns. Viruses can knock out power stations, pound locks can be manipulated remotely and a Boeing 747 can be taken over from a passenger seat.

WHAT SHOULD THE GOVERNMENT DO?

1. Introduce the right economic incentives. Companies should feel it financially if their security fails: financial motives convince decision-makers like no other, particularly in a commercial organisation.
2. Offer active help. The government needs to assist sectors such as energy, air-traffic control, hospitals and nuclear installations. At these locations the government could, for example, monitor networks to detect any large-scale virus attacks or espionage. Good legislation would certainly be needed to protect privacy.
3. Cyberspace enforcement needs to be given teeth. In the real world the police carry weapons, but in cyberspace everyone is equal. It's almost impossible to arrest criminals who live in country A and steal money in country B using servers in country C. Collaboration is indeed needed at all sorts of levels, such as the EU, NATO and the UN. However, we could already make a start at the national level.

Once we have organised the issues above, it will again be time to engage in the battle against cybercrime. You can win a battle but still lose a war. ■

Ronald Prins, Fox-IT CEO

Defence works securely from home via OpenVPN

Fox-IT has improved the security of the open source VPN software package OpenVPN. The National Communications Security Agency (NBV) of the Netherlands' General Intelligence and Security Service (AIVD) has approved the product in that it meets the high security requirements of the Ministry of Defence. Ministry employees can now use this VPN connection to work securely from home.

'Many security products are poorly constructed,' notes Wouter Teepe, product manager at Fox-IT. 'The NBV separates the wheat from the chaff and only grants its approval to very few packages. Manufacturers themselves also have to prove that their package is secure, which takes an enormous amount of time and money. Most companies are not prepared to make those investments. An open source package is often produced by volunteers, and they have absolutely no interest in doing this.'

FOX-IT MODIFIES OPENVPN

There certainly was a demand for OpenVPN within the Dutch Ministry of Defence – an open-source solution for the secure and encrypted exchange of information between two locations or networks, enabling secure working from home. 'Alternative solutions are costly,' says Wouter Teepe by way of explaining Defence's preference. That's why the NBV asked Fox-IT to improve OpenVPN such that it would get through the approval process successfully. 'We had to act as though we were the developers of the package and modify the software so that it met the NBV requirements.' On this basis the NBV conducted an evaluation and then approved OpenVPN-NL.

Defence has a number of security levels for confidential information. 'OpenVPN-NL had to at least comply with the "Restricted" classification level. More than 90 per cent of Defence's confidential information falls within this classification. Should such information leak out unexpectedly, then the damage for the state would be manageable.'

OPENVPN IMPROVEMENT PROCESS

Fox-IT undertook a variety of actions to convince the NBV that OpenVPN-NL is secure. Wouter Teepe: 'First we detailed the structure of the software through documentation. We indicated what each piece of code did.' Fox-IT also improved parts of the product. 'For example, we mounted a different cryptographic engine under it, PolarSSL instead of OpenSSL. This makes the connection much more secure now.' Fox-IT also arranged a reliable distribution channel: people can download the modified version of OpenVPN-NL from a part of the Fox-IT website with cryptographic signatures. 'In this way the user can be certain that he is downloading an approved product.' The improvement process was completed in the autumn of 2011. ■

PILOT WITH TELESTICK

In the summer of 2011 the Ministry of Defence conducted a pilot project with OpenVPN-NL. Employees were given a telestick, a type of USB stick containing the software. This enabled them to log into the Defence network from home, and to work securely. Wouter Teepe: 'The pilot run was successful and the staff were extremely enthusiastic. For example they could read their e-mails or could record their leave days. Very handy for employees who don't have an office job. Defence will be using OpenVPN-NL fully from this year, including for confidential information.'

British government deploys DataDiode for data protection

SECURE ONE-WAY TRAFFIC

From the internal revenue service to customs and from the police to nuclear power plants, many bodies operate with sensitive information. How do you ensure that this information doesn't leak when exchanging data? FCO Services, part of the Foreign and Commonwealth Office, deploys the DataDiode developed by Fox-IT and supplied by UK OEM partner Nexor, as part of the solution. This guarantees that information can only flow one way.

The British Government has decreed that all its departments must ensure greater security for sensitive information. Where data loss would cause serious embarrassment or compromise security, firewalls offer insufficient protection. A software solution such as a firewall certainly does filter information coming from an external network, but it is also vulnerable to the possibility that sensitive information will flow the other, 'wrong', way. Cybercrime or sabotage cannot be entirely ruled out as a result.

RIGOROUS DATA PROTECTION

For FCO Services, this was the motivation to seek a solution that guaranteed only one-way traffic: information must only be allowed to flow to the rigorously protected FCO Services network, and not the other way. This strict data protection is vitally important for FCO Services as they design, build, integrate and support secure ICT systems that meet the demanding standards of CESG, the UK National Technical Authority for Information Assurance, and other government bodies for use by the Foreign Office and the wider UK government community.

'FCO Services approached us in 2010 whilst they were evaluating data diodes,' explains Humphrey Browning, Business Development Manager at Nexor, a leading British provider of information security solutions for government and critical national infrastructure. 'As a Fox-IT OEM partner we were able to offer an enhanced security solution making use of the Nexor Data Diode and our experience and expertise in building secure information exchange solutions'

REAL-TIME ACCESS TO INFORMATION

'FCO Services wanted to allow centralised management of the networks they support,' explains Browning. 'This meant audit and monitoring information from all the networks needed to be transferred securely and as quickly as possible to the management domain.' With an air-gap (see sidebar, ed.), this cannot be done. 'We made it possible by deploying several Nexor Data Diodes in combination with software we developed around HP Operations Manager, one of the most widely used system management applications in large organisations worldwide.' FCO Services wanted to ensure this data was passed between networks in a secure manner via HTTPS, which is in fact a two-way connection,' notes Browning, 'so we had to turn this into one-way traffic. A difficult task, but with the Nexor Data Diode and a specially developed proxy application we were able to offer a secure solution.'

SATISFIED

'Throughout the project, we worked closely with FCO Services. In the early stages, we understood their requirements and helped to prove the concept they had in mind. We then used the Nexor Data Diode enhanced with software for FCO Services' specific needs,' recalls Browning. 'After the installation, we provided two days of training for FCO Services staff to enable them to be self-sufficient in day-to-day operations of the solution.'

FCO Services has indicated it is extremely satisfied with the solution. 'We are particularly pleased that we now have access to information from other networks in near real-time,' said an FCO Services spokesman. 'We are also happy that the installation went without a hitch.' And adds Browning: 'Nexor and FCO Services continue to work together on the back of this success and we look forward to using the DataDiode as the basis for further enhanced security solutions in the future.' ■

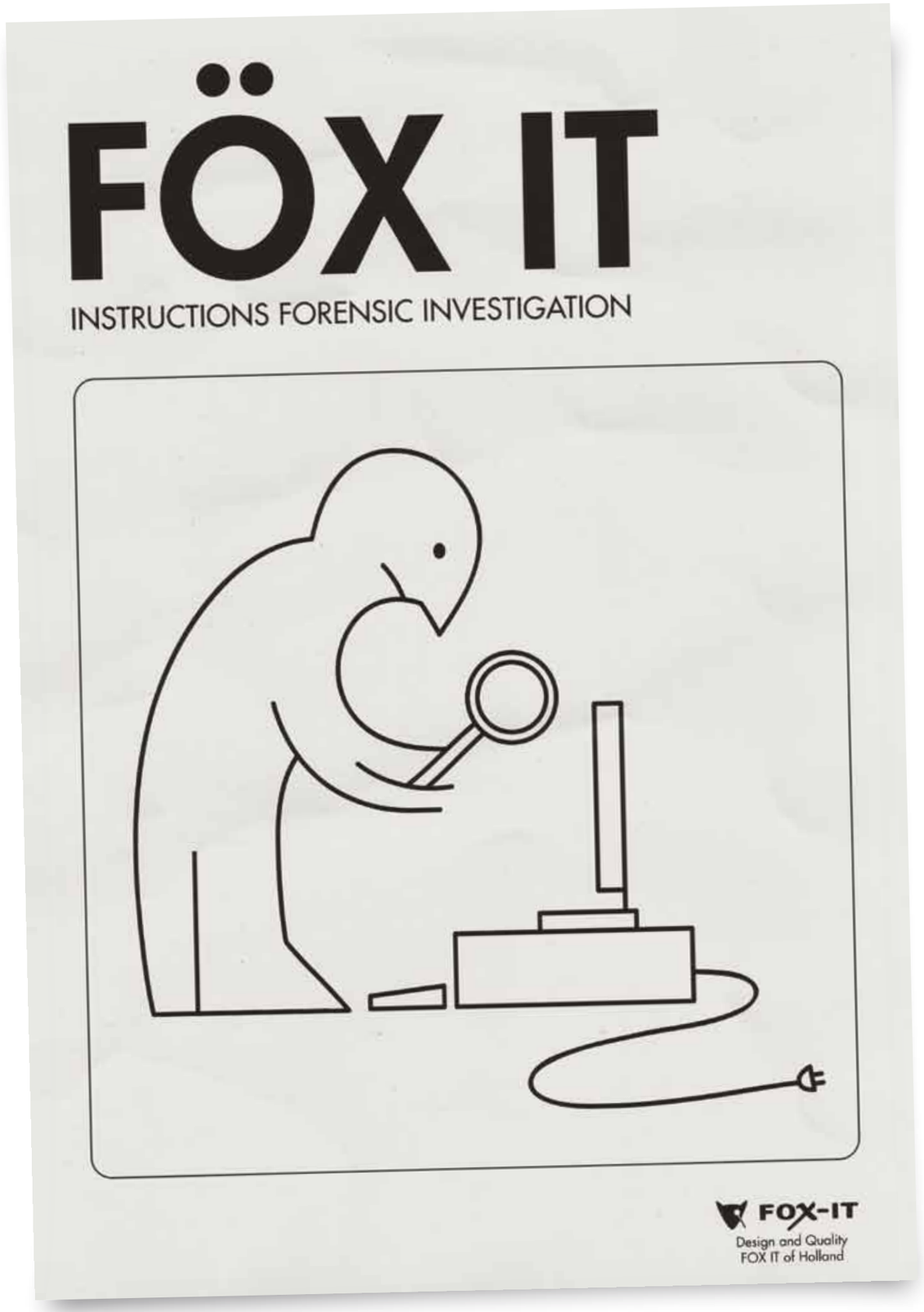
A DATA VALVE OFFERING CERTAINTY

'The DataDiode is a data valve which ensures that information can only flow one way,' is how Wouter Teepe, Product Manager at Fox-IT describes the solution. 'The DataDiode offers far more certainty than a firewall, whose two-way traffic means information could leak out. This two-way-traffic problem is often resolved with a so-called air-gap, in which a network with a high security level and one with a lower security level are separated. But this doesn't work optimally. In such a case information exchange occurs using a CD or a memory stick, which is sensitive to errors and can get lost or be stolen. The DataDiode makes transport media superfluous.'

The DataDiode has been approved by the AIVD (the Dutch General Intelligence and Security Service) for linking networks up to and including the 'Secret' classification level. NATO has accepted the DataDiode for use up to and including the NATO SECRET level. This means the DataDiode may be used as protection against any leakage of very sensitive NATO information. The DataDiode is also available for the private sector.

NEXOR®

Nexor specialises in secure information exchange for governmentand critical national infrastructure and has been an OEM (original equipment manufacturer) partner of Fox-IT since 2009. 'We first met Fox-IT at an exhibition,' says Nexor's Humphrey Browning. 'We quickly identified a close synergy and established an excellent working relationship which led to us becoming an OEM partner. We continue to collaborate closely to develop solutions for our chosen markets.'



Do-it-yourself
in forensic investigation

A new trend is emerging in the world of forensic investigation: increasingly, companies want to carry out digital forensic detective work themselves. Fox-IT offers a number of useful tools for this, such as the Fox Tracks Inspector and Clearwell. This now enables investigators, fraud specialists or lawyers with little digital forensic knowledge to quickly search through and analyse e-mails and other digital evidence themselves.

The volume of digital information is enormous. In the event of (suspected) fraud and cybercrime, digital forensic investigation is increasingly important for organisations. It can be time-consuming and costly to engage experts like Fox-IT for every instance. It's also much more useful if people who know a case intrinsically can also conduct their own digital forensic investigation. In a way that also meets all the legal requirements, because evidence you can't use in a legal case is pointless.

ESTABLISH THE LINKS YOURSELF

Fox-IT has developed a variety of tools, such as the Fox Tracks Inspector in 2010, with which organisations can analyse digital evidence themselves in a few minutes. The tool seeks out digital traces in storage media such as hard-disks, USB sticks and servers. Useful for police investigators, for instance. Marco de Moulin, Fox Tracks Inspector project manager: 'Generally, tactical investigators have limited digital backgrounds, which is why they often delegate computer investigation to a digital expert. But such experts have multiple investigations to conduct, so that you can join the queue and it can take a long time to get a definitive answer. Tactical investigators will also be quicker than digital experts to recognise connections if they can sift through the information themselves, because they are completely involved in the investigation. So reasons aplenty to keep the investigation with the tactical investigator as much as possible. With the Fox Tracks Inspector, investigators without a technical background can easily get to work themselves.'

> 'You make discoveries which might otherwise have remained hidden'

CLEARWELL: 80% TIME SAVING

For searching through e-mails, Fox-IT also offers since 2010 Clearwell, an e-discovery tool from the American Symantec company. Hans Henseler, e-discovery expert at Fox-IT: 'Clearwell has a lot of useful features enabling you to read and process e-mails more easily. That gives you an insight into an investigation in a couple of hours rather than a few weeks. For example you can combine e-mails on the same subject, or filter the senders. Or view just who has responded to who with a tree structure. You can then view the entire discussion at a glance, extremely comprehensibly. Clearwell also indicates key words that occur frequently, giving you a quicker idea of what you are looking for. All in all, using this tool results in a time saving of 80% over other search methods.' And the old adage applies here too: it's child's play, as it were.

RABOBANK SAVES ON EXTERNAL COSTS

Rabobank will be getting to work with Clearwell this year. Thomas Eekels, senior fraud and risk management advisor for the bank: 'We've already had a security department for 25 years with financial specialists, lawyers and investigators. From the Netherlands we investigate worldwide fraud within the Rabobank. Since 2008 we have also been involved in digital information security to combat cybercrime. That's

‘We prefer to leave cases with a high integrity value to the experts’

Thomas Eekels, senior advisor fraud and risk management at Rabobank

when our team was augmented with ICT people specialising in information security.’ Rabobank initially acquired Clearwell for compliance research. ‘Financial authorities subject us to enormous requirements. If they suspect that something is not quite right or needs more explanation, we are obligated to supply a whole lot of details. We used to outsource such an investigation to Fox-IT. Now with Clearwell, we no longer need to approach Fox-IT for every digital investigation, and we can operate decisively and more economically. "

NEW INSIGHTS INTO FRAUD INVESTIGATION

A nice incidental advantage is that the Rabobank can also deploy Clearwell for fraud investigation. Thomas Eekels: ‘We think we will be able to resolve more fraud cases with this tool, because Clearwell gives you new insights, so that you suddenly start thinking in an entirely different direction. You make discoveries which might otherwise have remained hidden. We get results more quickly if we conduct this type of digital forensic investigation internally, and the data remains within the Rabobank network.’

MAJOR INVESTIGATIONS TO THE LAB

Organisations use the Fox Tracks Inspector and Clearwell mainly for smaller investigations. Thomas Eekels: ‘We prefer to leave cases with a high integrity value, in other words those which will be presented to a court and/or end up in the media, in the hands of the Fox-IT experts. For example when we collect information for a court case in which we request the dismissal of an employee who has perpetrated fraud. Then the evidence has to be rock-solid. Investigative results from an independent Fox-IT forensic investigator certainly carry more weight then.’

SUPERLAB

Fox-IT recently acquired a new laboratory with the latest research equipment. Hans Henseler: ‘Because companies can do more forensic investigation themselves, we see that we can focus more on major, complicated investigations. So an advanced research environment is needed for that.’ In the future Fox-IT would also like to enable companies to undertake major investigations themselves. ‘We are considering the possibilities of setting up such an advanced laboratory for major companies, or advising them on it.’ ■

GETTING TO WORK YOURSELF?

Fox-IT offers practically-oriented training on conducting digital forensic investigation.

- **Basic training in digital forensic investigation**
  Five-day training course on all aspects of digital forensic investigation: the technical, tactical and legal aspects.
- **Digital forensic investigation in a Microsoft environment**
  Four-day training course in which specific attention is devoted to systems within a Microsoft network environment.
- **Digital forensic investigation in relational databases**
  Three-day training course on efficiently securing and analysing comprehensive and complex databases.

More information
See the training calendar on the back page or at www.fox-it.com.

I AM FOX-IT

‘I’m extremely obstinate’

FOX IT

Name	Kevin de Kok (29)
Position	Security Analyst
Training	Higher Vocational Diploma in Network Infrastructure Design / University Master’s in System and Network Engineering
Passion	Always in search of something new and challenging

Who are the people at Fox-IT who work for our safety, often at the oddest times? From what cloth must you be cut to be a Foxer? In short: Who is Fox-IT? Security Analyst Kevin de Kok in 10 keywords.

SOCIAL IMPORTANCE
‘Human lives are on the line with critical infrastructures. We help to protect them. I appreciate the fact that in my own way I make a significant contribution to the safety of our society.’

INNOVATION
‘Innovation is creativity. If you dare to reach far outside your own boundaries and knowledge areas, you will find the solution.’

CULTURE
‘I enter the building with a smile every day and I always get a smile back. That’s the atmosphere which pervades here. We work informally with each other, and trust and integrity are high on our checklists.’

NERD
‘Sure! I want to know why things break or how you can break them; it’s a game. But at the same time I’m also very sociable.’

WORK ENJOYMENT
I’m open and honest, and that works here at Fox-IT. That’s how we all are. I think it’s extremely fascinating how everyone has their own view of things, that we keep puzzling away at something until we achieve one solution together.’

FREEDOM
‘We have an enormous amount of freedom here. The location does not determine the work that we do. If I jump up awake in the middle of the night with a solution for something, then I work it out immediately. And then I don’t have to wander into the office until two the next day. Ultimately you simply have to complete your work. How and when you do it is up to you.’

OBSTINATE
(Laughs) ‘Yes! I’m extremely obstinate. I have my own opinion and I’m critical.’

ADDICTION
‘I was addicted to gaming for a long time, and I even ended up in social isolation. Until I started getting terrible nightmares. Then I switched 180 degrees. I don’t game anymore.’

LOOKING FORWARD
‘Change happens so quickly that I wouldn’t dare make any predictions about my career. Perhaps I will indeed do something involving advising or teaching in my specialist field. In any case I hope to stay healthy and happy for a long time.’

FOXER BECAUSE...
‘This is a pleasant environment where you can be 100% yourself.’ ■

Do you recognise yourself in Kevin and does the Fox-IT work and culture appeal to you? Then go to www.werkenbijfox-it.nl and bit.ly/foxmanifest.

News and **agenda**

‘Mobile Device Security’ seminar

People are using their smartphones and tablets increasingly for accessing and sharing sensitive corporate information. This type of working on the move raises a number of issues within organisations in the search for a balance between user-friendliness and security:

- What technical measures are needed?
- Can a ‘Bring Your Own Device’ policy be secure?
- Where are the risks of data leaks?
- What are the legal risks? And how do you adapt your policy to these?
- How do you deal with incidents and how do you prevent them?
- What’s the malware situation for Android and Apple iPhones/iPads?

On 25 April Fox-IT is organising the ‘Mobile Device Security’ seminar to answer these questions. This gathering will be interesting for anyone in an organisation involved in the implementation and protection of mobile working, such as security officers, fraud researchers and policy staff for both companies and governmental organisations.

More information and registration: www.fox-it.com

Seminar	Mobile Device Security
Date	25 April 2012
Venue	De Lindenhof, Delft
Times	13:00 to 16:30, followed by refreshments until 17:30
Cost	€ 195 p.p. excl. BTW/VAT

For attorneys and lawyers:

ONLINE FACTS RESEARCH

On 23 May Fox-IT is launching a training course for attorneys and lawyers. Participants will learn relevant information about gathering and verifying information about people and companies on the internet, and the legal establishment of the results. Taking part in this varied theoretical and practically-oriented training course entitles the participant to 10 VSO/PO points. More information and registration via www.fox-it.com.

Securely on the move

A Fox-IT team is working on a toolkit, with which developers can implement security measures in their apps for mobile platforms. Read more about it in the next FoxFiles.

TRAINING CALENDAR

Online Research

26 to 27 March	Investigation on the Internet (IoI) – Follow-up training
16 to 19 April	Investigation on the Internet (IoI) – Basic
23 and 24 May	Online Facts Research for Lawyers

Digital Forensic Research

14 to 16 May	Digital Forensic Investigation – Relational databases
11 to 14 June	Digital Forensic Investigation – Microsoft environment
18 to 22 June	Digital Forensic Investigation – Basic

Product Training

02 to 03 April	International Research Network (iRN) – Basic training
23 to 25 April	International Research Network (iRN) – Advanced training
07 to 08 May	International Research Network (iRN) – Basic training
09 to 11 May	International Research Network (iRN) – Advanced training

More information: www.fox-it.com