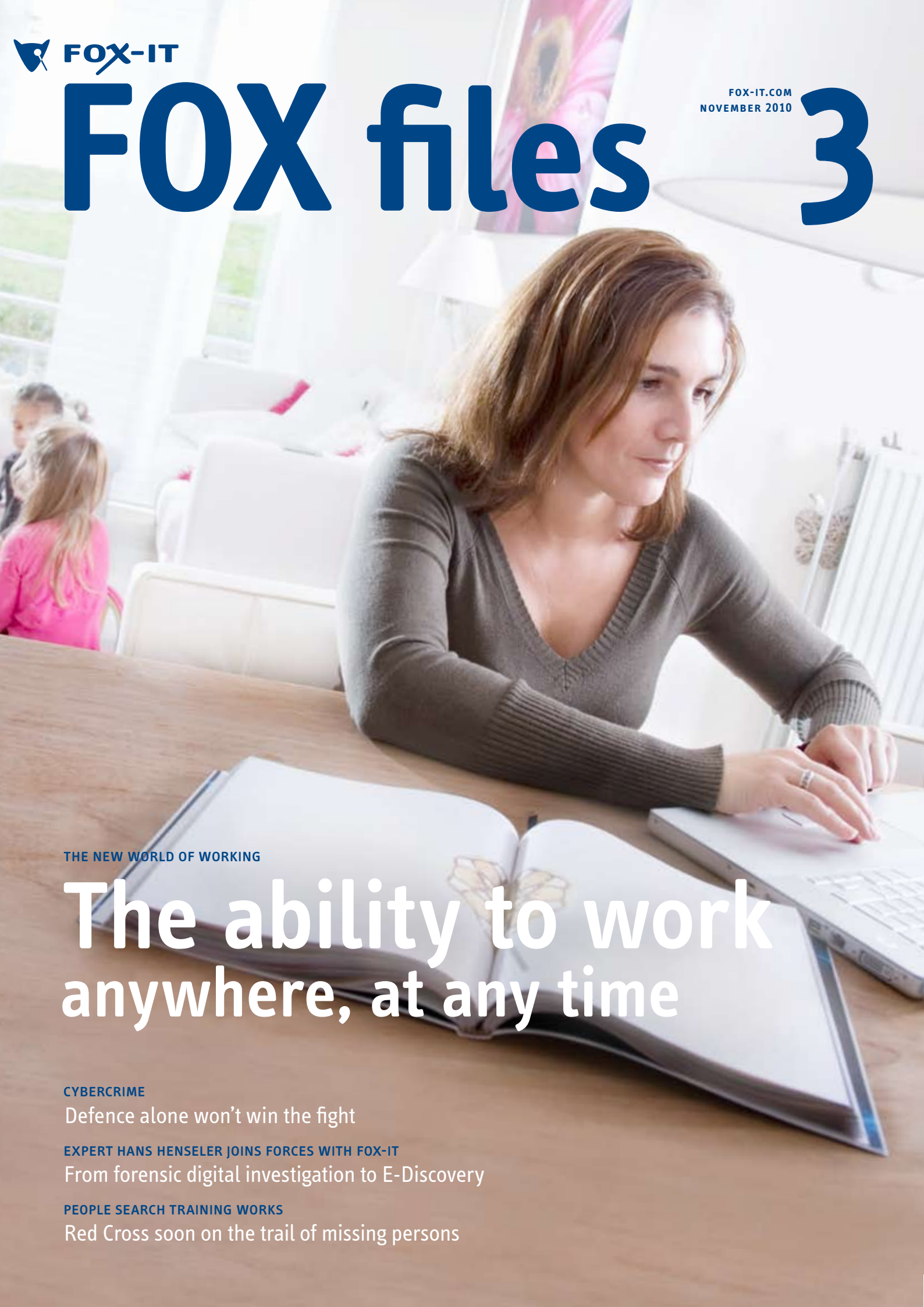
FOX-IT

FOX files 3

FOX-IT.COM
NOVEMBER 2010



THE NEW WORLD OF WORKING

The ability to work anywhere, at any time

CYBERCRIME

Defence alone won't win the fight

EXPERT HANS HENSELER JOINS FORCES WITH FOX-IT

From forensic digital investigation to E-Discovery

PEOPLE SEARCH TRAINING WORKS

Red Cross soon on the trail of missing persons

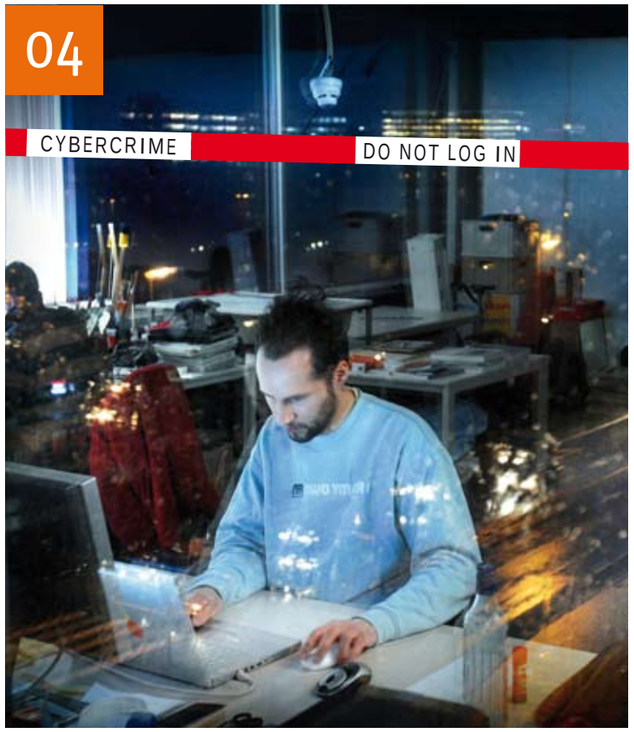
16


10


24

18


21



04

COLOPHON

Editorial address
Fox-IT Marketing department
PO Box 638
2600 AP Delft
The Netherlands
+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 texts
Sabel Communicatie, The Hague

COLUMN

Ronald Prins, Director

Who's the boss?

Who's the boss? Normally we know the answer. Every area of our lives is governed by rules telling us how to behave. And if we don't behave, there are consequences. At school, it's a teacher, at work it's your manager, while on the motorway the traffic police will flag you down if you flout the Highway Code.

But that system doesn't work on the internet. There is no internationally accepted code of conduct. There is no boss or supervisor. The internet has become big and successful thanks to the lack of clear rules.

Obviously, it's difficult to translate our laws from the physical world into the digital domain. However, we try. We already have two computer crime laws and a third is currently in the pipeline. An important element in this new law is that now a public prosecutor is explicitly authorised to remove a website from the internet if it contains information that constitutes an offence.

The internet community has responded rather negatively to this. Many people do not feel that a public prosecutor is the right person to assess whether a website is actually distributing information that constitutes an offence. They feel it should be a judge. The concern is that a public prosecutor might intervene too quickly in cases of criminal defamation (slander, incitement, etc) and thus restrict freedom of expression and opinion. I don't want to pursue this argument here, but it does show how difficult it is for the government to approach rule enforcement on the internet.

Another frequently voiced opinion is that there should be more intervention. After Stuxnet became headline news, the cyberwar or cyberterror threat has become more widely acknowledged. More and more frequent incidents of cyber-espionage are being discovered.

Continued on page 14 ▶

CYBERCRIME

Not my concern?

CYBERCRIME: THE NEW REALITY

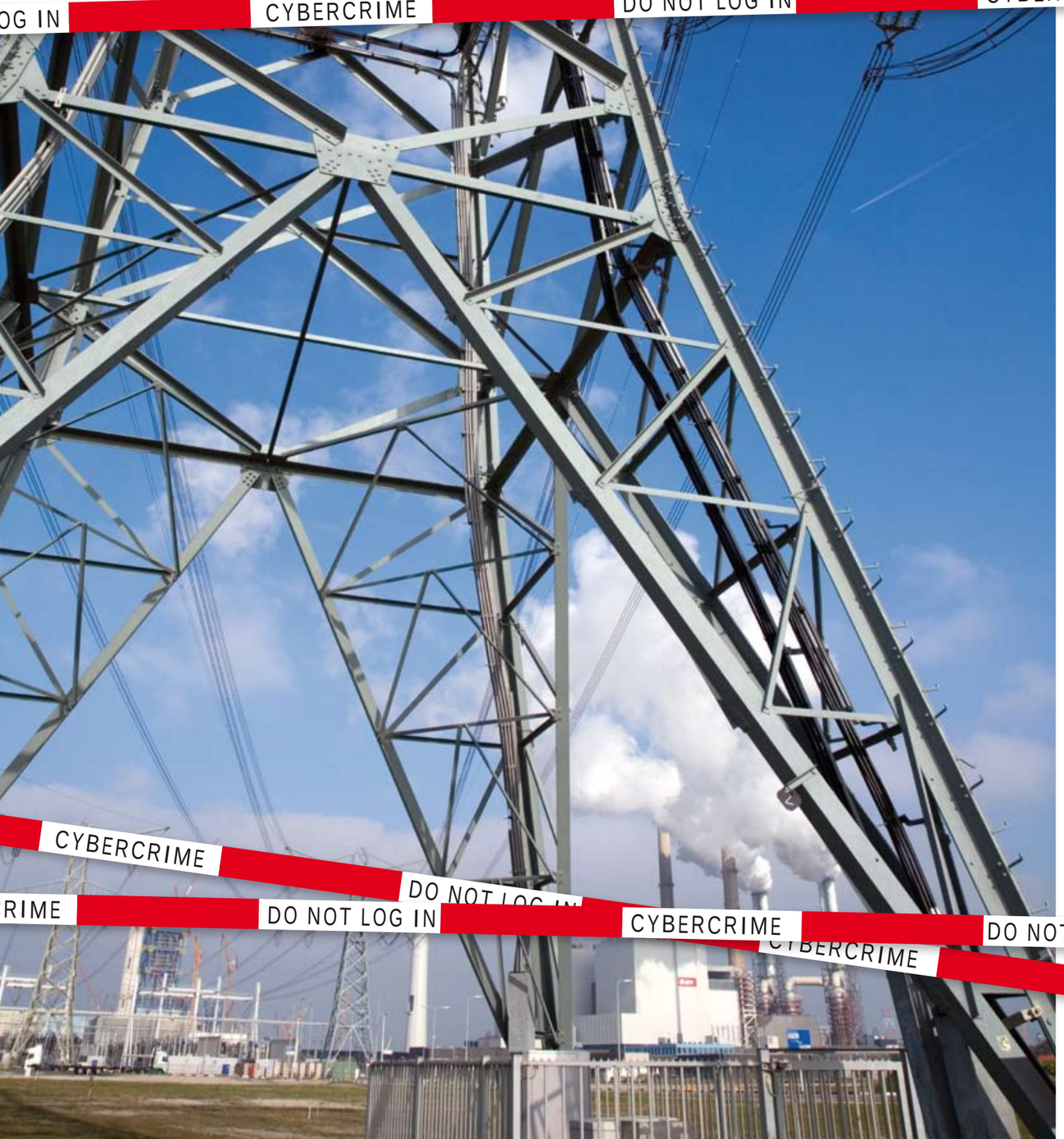
The Stuxnet attack in Iran at the end of September, bank accounts hacked through internet banking, a critical website crippled: we read about such incidents every day. Yet many organisations assume they are safe when it comes to securing their crucial business data. After all, they have a firewall and they've invested huge amounts in security. Yes, you need to defend yourself, but you also need to detect threats.

DO NOT LOG IN CYBERCRIME DO NOT LOG IN CYBERCRIME

CYBERCRIME

‘Fox-IT enters the battle against cybercrime’

Organisations which are stuck in their old framework forget that the world is changing



Technology is developing fast. Very fast. Cybercriminals are quick to latch on to these developments. They are now IT experts who can easily access and pass on business-sensitive information to competitors via the internet. These criminals benefit from the low security awareness of people and organisations. The exponential growth of cybercrime therefore demands a new approach to security.

NEW CYBERCRIME UNIT IS ENTERING THE FRAY

Fox-IT’s new Cybercrime unit aims to get under the skin of the cybercriminals. In this unit, Fox-IT combines all its cybercrime-related expertise. Every day, twenty-five security experts swing into action to prevent, monitor and resolve damage and theft of business data. Director Menno van der Marel, business unit manager Jeroen Herlaar and project manager Eward Driehuis are united in their approach: security can no longer be viewed from inside your own castle. Just putting up barricades is no longer enough. The internet has penetrated every aspect of life. Cybercriminals have become professionals. The advance of ‘emerging markets’ presents new risks. Fraud, hacking, espionage and information theft is on the increase. Menno van der Marel: “The combination of these aspects requires a new mindset with regard to the security of business data. There are many more areas to think about as a company. Particularly if the internet component is substantial or there is major investment in intellectual property. With the new Cybercrime unit, we can apply our knowledge much more quickly and effectively for our clients.”

FROM HACKER TO SPY

Fraud and hacking are forms of cybercrime which have the attention of business and criminal investigation services. Recently, two Germans were caught intercepting EUR 2.3 million from European, American and Thai bank accounts. Less well publicised but a growing international problem are espionage and terrorism. Cyberspies look for and find sensitive business information to sell on to the competitor; cyberterrorists cripple systems, disrupting critical infrastructures. Big organisations and governments continuously need to improve their armoury.

STAYING IN CONTROL

The focus is shifting from technology to information. In the past,a secure server and laptop were the main issues. With the arrival of cloud computing and SaaS, the location of information is not always clear. So how can it be secured? “Businesses must take a different approach to their security strategy,” Jeroen Herlaar explains. “That demands a very specific expertise to be able to see potential threats. Building and maintaining a security structure is not enough. You need to consider questions like: where is my information? How is it distributed? What online activities is my company involved in? How do threats develop? What risks do I accept? What methods are there to stay in control? Who communicates, accepts that information can be published? You then need to be certain that the information is only used where it is needed. And that there is a good response mechanism if anything goes wrong. This requires totally different security methods than in the past.”

LEADING THE FIELD

If you’re always on the defence, you’ll never win the game. “One of our added values for clients is that our experts are very well informed about what goes on in the digital underworld, where the threat originates from. So we monitor forums where hackers often meet and we even take part in chat sessions. We need to understand what is happening there and what the new modus operandi is. Many of our experts have a hacker’s background and are well qualified to interpret the information they find as threats.

Criminals work in layers. There is a layer which builds the criminal infrastructure, a layer which builds malware, a layer which passes on the money and a layer which wants to earn the big money.
These layers come together in so-called trading places.

By monitoring them, we know what's going on and have a good idea of the risks to which our clients are exposed. This new approach means we are more in control. Our signalling methods and in-house knowledge enable us to raise our clients' security level."

EFFECTIVE SECURITY MEASURES

In order to put together the right mix of security measures, we need to analyse the threats to the organisation. The biggest threats often target valuable information. The next step is to determine the risks of these threats. What would be the consequences if a certain threat became reality? What would be the damage if this information was stolen? An important element here is always to put the goals of the organisation first.

The third step is to put together a mix of security measures. The layered approach of the cybercriminals can only be countered with a layered security approach, or 'defence-in-depth'. Eward Driehuis explains what this looks like in practice. "You can't trust in a security measure always working. It is often advisable to take extra measures as a back-up. You must protect vulnerable parts of the organisation and infrastructure, the areas where the information is contained."

Detection is the fourth component. An organisation may never assume that the security is 100%. Information is transient and you therefore have to monitor the situation, from the inside too, and detect unauthorised traffic. Finally, you must be able to respond to incidents. Even if something bad happens, the day-to-day business must continue. We then collect evidence and show our clients exactly where they are vulnerable. Our Incident Response Teams are quick to act."

A NEW MINDSET

Organisations which are stuck in their old framework tend to forget that the world is changing. Jeroen Herlaar: "Sometimes we conduct a penetration test whereby we easily manage to breach the security. Companies do invest - huge amounts - in security, but they take measures which their own ICT department knows. And these tend to be defensive. They don't have the mindset of a hacker and therefore fail to recognise the risks and threats."

"And another thing," Menno van der Marel adds, "companies don't realise the simplicity of technological possibilities. Spyware can be distributed through a USB stick left lying around. Once you unsuspectingly plug it into a computer, the damage is done. Access a company through the CEO? No problem. You look on his LinkedIn page, find out what conferences he attends and what his e-mail address is. This CEO then receives an e-mail from a 'professional' party which looks reliable. This contains an 'interesting' link about the conference he has just attended. After clicking on the link, the system is infected. As a result of the CEO's (unfounded) trust in the sender of the message, criminals have access to valuable information. We therefore feel it is important to make clients aware of targeted attacks by cybercriminals." ■

CYBERCRIME, THE DAILY REALITY

Is today's news tomorrow's chip paper? Not when it comes to cybercrime. The following examples prove the contrary.

- An academic hospital is the target of a huge malware outbreak. The virus scanner cannot cope with the attack and for a moment even threatens to disrupt treatments. The tide is only turned after the intervention of Fox-IT. Nevertheless, the hospital's processes are disrupted for a whole week.
- The Stuxnet worm ushers in a new phase: malware now targets specific industrial processes. In Iran, an entire nuclear plant is down. Because the worm is distributed through USB sticks, the usual industrial network firewall is not enough. Whoever is behind this work, and whether it is a targeted attack, is subject to speculation. What we do know is that it is an organised attack.
- An insurer falls victim to a targeted attack. The goal? To bring down the websites. For several days the insurer is able to offer only a few of its online facilities. The organisation suffers financial damage and clients experience a great deal of disruption.
- During a periodic penetration test of an energy supplier, Fox-IT discovers serious vulnerabilities in the network. Even more serious: these vulnerabilities had already been used. There is evidence of previous hacks: the trails point to China.

People don't have the mindset of a hacker, so they don't recognise the risks and threats

FOX-IT AND HENSELER FORENSICS JOIN FORCES IN FOX-IT FORENSICS

‘Digital proof goes further than e-mail’

HANS HENSELER

Hans Henseler studied computer science at Delft University of Technology and completed a PhD at Maastricht University in 1993 on “artificial neural networks and pattern recognition”. A year previously, he had set up the Forensic Computer Investigations department at the former Forensic Institute (today this is the Digital Technology department at the Dutch Forensic Institute - NFI). From 1998 to 2000, Hans worked in the Information Systems division of TNO TPD, the independent Dutch scientific research organisation, where he worked on commercial applications of image processing, language technology and knowledge management, among others. Until the end of 2006, he was then technical director of the company ZyLAB where he was responsible for the development of software for document and record management and E-Discovery. From 2006, Hans worked at PricewaterhouseCoopers Advisory (PwC) in the Dispute Analysis & Investigations department. As director of Forensic Technology Solutions (FTS) at PwC Eurofirms, he was responsible for acquisition, implementation of research and the development. Since 2009, Hans has lectured part-time in E-Discovery at the college Hogeschool van Amsterdam, and in 2010 he set up his own business, Henseler Forensics.

Fox-IT and Henseler Forensics have combined their forensic activities in Fox-IT Forensics. Who is Hans Henseler, why did he choose Fox-IT and when will you come across him?

Hans Henseler (1964) is the founder of Henseler Forensics and lecturer in E-Discovery at the college Hogeschool van Amsterdam. Since 1 August 2010, he is also the managing partner of Fox-IT Forensics. In this capacity, he is responsible for the management and commercial development of the forensic activities. He also continues to be a strategic advisor and account manager involved in innovation and business development related to digital forensic investigations.

OWN BUSINESS

Early this year, Hans took a new and challenging step in his career (see box): he started his own business: Henseler Forensics. Since August, Fox-IT and Hans’ company have been working together on deepening forensic digital investigation within Fox-IT, widening service provision in the market and strengthening business relations. “I have a lot of experience with the synergy that can be created between financial experts such as forensic accountants and digital specialists,” says Hans. “That is precisely the reason why Fox-IT and my company are such a good match. With my knowledge and experience, Fox-IT can optimise its services and thus respond better to the opportunities and needs in the market.”

FASTER PROOF WITH BUSINESS PROCESSES READY FOR INVESTIGATION

“Digital investigation is more than just checking e-mails and hard drives,” Hans continues. “With E-Discovery, everything is interdependent and there are digital trails everywhere. One example: when an employee commits fraud by making money disappear, this should be reflected in the bookkeeping. Often the money is booked to inconspicuous posts. These leave their traces in the invoice and payment flows. It’s important that a financial trace investigation can be combined with other digital investigation. When organisations ensure that their business processes are ready for forensic investigation, it’s easier to start a digital investigation, proof is more easily found and you often have more data. Furthermore, the costs of the investigation are much lower and normal operations are not disrupted.”

LOOKING FOR CHALLENGES AND SOLUTIONS

“What can clients expect from me? I look forward to entering into a discussion with them. I want to innovate and translate their challenges into solutions and prepare them to meet these challenges.” Hans also applies this focus on solutions outside his work. “I travel a lot and I love to read when I’m on the move. I’ve just finished Stieg Larson’s Millennium Trilogy. They are great stories, and not just because they are about digital espionage and fraud. They are exciting and logically constructed, whether they’re true or not.” ■

Safety doesn't stop at the border

FOX-IT GOES GLOBAL

Fox-IT's mission is to make society more secure. This goes beyond the Dutch borders. The company is also active abroad, together with reliable partners and with innovative products like the Fox DataDiode and FoxReplay Analyst.

Fox-IT was founded in 1999 and has since experienced a phenomenal evolution. In the early years, a limited number of services were offered by a small group of specialists. As time progressed, these developed into a portfolio of extremely specialised products and services, built up by a steadily growing number of staff. They develop solutions to protect confidential information, conduct intelligence agencies, fight cybercrime and produce analysis products for tracing services. Fox-IT has a strong focus on innovation and wants to continue growing. Also outside the Netherlands.

TRUSTED PARTNERS

With its products, Fox-IT helps many clients, such as governments, defence organisations, intelligence agencies and socially important institutions. These organisations handle extremely confidential information on a daily basis. In order to protect themselves from criminals, they work with a small group of suppliers and partners: 'trusted partners' who have proven themselves in their own country. Fox-IT has already achieved this status in the Netherlands. Beyond the borders, however, it is very difficult to achieve the status of trusted partner. For this reason, Fox-IT works with local partners: partners who are trusted to protect sensitive, confidential information and who, like Fox-IT, are striving to create a safer society.

SELECTION PROCESS PARTNERS

Fox-IT's partners must fulfil a number of criteria. They must be specialised in IT security and supply similar services and products in their own country. Furthermore, the partners must also be able to implement and maintain Fox-IT's products. Because Fox's reputation is important, it expects the same quality from its partners. Good partners are therefore difficult to find.
At the moment, Fox-IT is represented by partners in the Middle East and the United States, among others. The company has its own offices in Delft, in the Caribbean and in the UK. Thus Fox-IT is now one of the most specialised, innovative businesses in the world, in terms of both security and digital criminal investigation.

Fox DataDiode

The Fox DataDiode is the highest evaluated product in the world (the Common Criteria EAL 7+). This special diode links two networks with different security levels via a one-way connection. This prevents data from the high level secure network being sent, openly or secretly, to the low level network.

INTERNATIONAL SUCCESSES WITH FOX DATADIODE

Although Fox-IT has only been operating on the international market for a relatively short time, it has already had some significant successes. These include projects in most European countries and in the Middle East where the Fox DataDiode is used.
A recent example is a project where Fox-IT and partner GSN (Global Security Network) implemented the Fox DataDiode for an intelligence service. This client wanted to open up two data sources with public information and connect them directly, real-time, to a central database with confidential information. The limiting condition was that it had to be impossible to leak the data from the central database. It was also important that this connection should always be available (24x7), that the data could be checked for errors and that the data is transmitted in a relatively constant but high bandwidth.

The Fox DataDiode proved to be the crucial component in the solution offered. Zayed Alji, Regional Sales Manager of GSN: "The delivery and implementation were part of a total solution, which was completed strictly within the time frame and budget. The Fox-IT team did the job with the expected expertise, discretion and due diligence."

ALSO FOR ORGANISATIONS WHICH OPERATE INTERNATIONALLY

Together with its international partners, Fox-IT is also an interesting party for many organisations working with very confidential information. Not only to help these organisations locally and internationally, but also to provide solutions to issues which are literally transnational. Because it is obviously impossible for companies operating transnationally to divide their security issues into national components. So anyone who thinks and works on a wider scale thinks of Fox-IT. ■

More information: Dirk Peeters, Vice President Business Development, tel. +31 (0)6 - 42 55 59 02

FOXREPLAY ANALYST

FoxReplay Analyst is the first choice in the field of Internet LI (Lawful Intercept) of many police and intelligence agencies all over the world. This Fox-IT product interprets intercepted internet traffic and reconstructs all communication, making it easy to analyse. The data is presented in the original form and sequence so that it is possible to see exactly what the target saw. With FoxReplay Analyst, analysing intercepted internet traffic is no different from analysing intercepted telephone calls.

Who's the boss?

Cybercriminality has existed for some time, but we are now witnessing an explosive growth. Young criminals, often from Eastern European countries, can earn thousands of Euros by manipulating bank transactions. Here too it is important that the government takes measures. However, this requires different authorisations than currently permitted in the new Computer Crime Act. An important way of tracking cybercriminals is the possibility to be allowed to break into their computers. Even if these computers are abroad!

A third Computer Crime Act is currently being developed

In order to stop botnets like Stuxnet, it is important to assume control of the Command & Control servers, for example. Besides stopping the activity of the botnet, it is then easier to investigate the offenders, those who are behind it. The problem is that tracing often stops at the national borders. Also, Dutch police are not (yet) authorised to perform hacking as part of their tracing activities.

As I write this, I am at a congress in the United States along with many people from the Cyber Division of the FBI. Now, the Americans often have a certain view of the world that we may not necessarily agree with. But in this case, I understand their argument: if our US citizens here in this country are affected; if it concerns botnets which take our money out of the US; if I can access it from the US, then I would say that the entire botnet is in the US and I am authorised to take it down. Of course the US tries to work together with other countries as much as possible. However, they are not all as cooperative as the Netherlands. The criminals realise that too and naturally seek out the countries where it is more difficult to reach agreement.

All in all, I feel it is high time that we launch a public discussion about how we can get and maintain security on the internet at an acceptable level. If our government also wishes to play a role in this - and I feel this is important - it will have to show that it takes this problem seriously. It will have to recognise, for example, that current legislation gives Dutch police very little scope to fight cybercrime. If we do nothing, the same people who worked on the success of the internet might now assume the enforcement too...

Ronald Prins, Director

THE DUTCH RED CROSS IMPROVES ITS TRACING SKILLS

Family members reunified thanks to the internet

Finding a long lost relative, after a divorce, adoption or emigration; this is a scenario we are familiar with through TV programmes that try to reunite family members. The Dutch Red Cross also looks for missing persons. Thanks to Fox-IT training, they can improve how they use the internet.

One of the tasks of the Tracing and Support department of the Dutch Red Cross is to trace lost relatives. Blandine van Schelven works in this department. "We try to reunite family members who have lost contact for personal or social reasons. It might be that someone's parents got divorced thirty years ago and the father lost contact. Or contact might have been broken by adoption or emigration." In the search for lost relatives, the internet plays an important role as a source of information. At Fox-IT, Blandine van Schelven followed the People Search training. "As a result of the training, our department is even better able to use the internet."

INTERNET: WEALTH OF ADDITIONAL INFORMATION

Van Schelven and her colleagues receive around 250 requests to trace missing people every year. "To trace people, we can apply to the municipal personal records database (GBA). We are authorised to request information from the GBA, but we must naturally safeguard the privacy of people we are looking for. The emergence of the internet means a wealth of additional information for the Dutch Red Cross. If substantial amounts of information are missing in the tracing request we receive, we can supplement them with data from the internet before we apply to the GBA. Also if people are no longer registered with the GBA, because they have moved house and have not registered at a new address, the internet is vitally important."

MAXIMUM SEARCH RESULTS

"We naturally want to get the most out of our investigation. internet can support us in this. Fox-IT's training 'People profiling using open sources' and which search terms give you the best chance of success. For me, the Mega Search Engines like Docpile are a real eye-opener. They give you many more hits when you search on a name. The various Google operators are also very useful: they enable you to filter all the search results with information which is specifically interesting to you. I have also found lots of useful sites outside Hyves and Facebook which can help you trace people more easily."

ENERGY AND INSIGHT

Van Schelven is very positive about the training: "Not just because of the new skills and knowledge I have acquired, but also because it has provided confirmation that we are already on the right track with our tracing techniques. And that's obviously good news. I found the training very refreshing: I acquired new energy and insights. I haven't yet solved any cases with my new skills, but that's because I have just completed the training. But I'm already able to search much better and faster on the internet!" ■

PEOPLE PROFILING USING OPEN SOURCES

The three day training 'People profiling using open sources' teaches participants how to find digital traces and other data which can help them trace people. The training provides great variety in practice and theory. In different modules, questions are answered like: which browsers are suitable for investigations on the internet and how should I use them? How do I remain anonymous during my digital investigation? Which information sources and news groups are essential? What support software is there? The training also looks at search engines, focusing on formulating the right investigation questions, choosing and combining key words in these questions and using the advanced search possibilities.

More information:
Michelle Holthuizen +31 (0)15 - 284 79 08

FOXREPLAY ANALYST

Efficiently analysing internet intercepts

Police and public prosecutors regularly monitor the online activities of suspects. These internet intercepts often generate valuable evidence, but they are time consuming and require specialist knowledge to study the coded data. FoxReplay Analyst facilitates the analysis. The police is already using the software and the first investigators have been trained. Forensic IT expert and tutor Christian Prickaerts explains.

Tap data direct to the workfloor

Bert Hubert, CTO of FoxReplay is delighted that the police have chosen FoxReplay Analyst. This is exactly what Replay was designed for: when we started its development, analysing internet intercepts was reserved for specialist personnel. Our aim was to make the intercepts accessible for teams of investigators. The police shows that our solution works. Robert van Bosbeek, head of the National Interception Unit (ULI) agrees: "The Netherlands is a pioneer in the centralised accessibility of tap material. Fox-IT's new software brings the material directly to the work floor, in an easily understood format."

Since time immemorial, intelligence and security agencies have been intercepting the telephone calls of suspects, looking for leads. In the last few years, it has also been possible to monitor suspects online, thus opening up a world of potential evidence. "There was one disadvantage," says Prickaerts. "Unlike telephone intercepts, internet intercepts of VoIP, chat sessions and websites, for example, generate coded data. A technical team first has to convert this information for the investigation team. For one tap lasting a month, that process took about 3 to 6 months. In order to speed up the analysis, we developed a new software package: FoxReplay Analyst. The first reactions are very promising."

SEE EXACTLY WHAT YOUR TARGET SEES

With FoxReplay Analyst, a technical investigator is able to easily analyse intercepted internet data. Without the support of a digi. The software interprets the data and converts it into clear language. Prickaerts: "All the internet activities of a suspect are displayed in the original sequence and form. Thus an investigator can see exactly when someone downloaded a document, forwarded it to someone else and talked to that person on MSN to enquire whether they had received the document. That sequence of events can be very important." An investigator can play back all the activities like a film and insert comments for colleagues in 'scenes' of interest. A technical person is only necessary in the event of ambiguities or unusual data.

TRAINING FOR THE POLICE

The Dutch police have recently purchased FoxReplay Analyst. Investigators can now analyse a intercept much faster. Yesterday's intercept can now be replayed immediately. This only takes them a couple of hours and they can obtain much more information from it. "The software is very easy to use," explains Prickaerts. "However, some search functions and filter options do require extra explanation. Particularly for people who grew up without the internet or who are unfamiliar with social media like Twitter, Facebook and LinkedIn." Fox-IT therefore provides training to police officers who will be using or maintaining this software.

LEARNING THROUGH SCENARIOS

Prickaerts: "Participants are first given information about the internet and how the medium works. Terms like IP address, domain names and web 2.0 are explained. They are then provided with some general information about FoxReplay Analyst. Our philosophy is that software is best understood by working with it. So a large part of the training consists of practical exercises." Prickaerts and his colleagues designed various scenarios for participants to work with. For example, they have to follow an drugsdealer who orders materials online and makes contacts through the internet. "During the training, participants discuss practical issues with us and ask questions," says Prickaerts. "This helps us adapt the software."

RIGHTS OF SUSPECTS PROTECTED

Information gathered by the police via intercepts may be used as evidence. "Privileged communication is an exception," Prickaerts emphasises. "What a suspect discusses with his doctor or lawyer, for example, may not be used in a case. When you intercept a suspect's telephone call and you hear his lawyer answer the phone, you put down the phone and delete the conversation." This is technically more complicated in the case of internet intercepts. FoxReplay Analyst enables users to mark certain activities as privileged communication. From that moment, the data is no longer visible and the session is deleted in the system. This ensures that we comply with the rights of suspects. ■

More information? Contact Christian Prickaerts, Forensic IT Expert at Fox-IT on +31 (0)15 - 284 79 08 or Prickaerts@fox-it.com

FOXREPLAY TRAINING

Fox-IT offers training to users and supporters during which you learn how to make best use of the software and achieve a result in the most efficient manner:

- In the Basic Training for Users, you learn how to use the most commonly used features of the system. Based on practical situations, you are challenged to interpret and process intercepted internet data. This training lasts 3 days.
- The one day Support Training is aimed at digital investigators who support tactical investigators in the use of Replay as part of an investigation. Participants in this training are assumed to have (ample) experience with digital investigation. Knowledge of and experience with analytical tools are also an advantage.

OPINION

Know the risks of social networks

"THE BAD GUYS ARE WHERE THE USERS ARE, AND TODAY, THAT'S THE SOCIAL NETWORKS"

Social networking sites are a new phenomenon. For some organisations and their personnel, these sites are very useful. A few would like to forbid or block their use. In my opinion, this is not feasible or desirable. But what are the risks and how do you deal with them as an organisation?

TIPS:

- Make your employees aware of the risks for themselves and the organisation.
- Advise your employees to choose a good, not obvious password.
- Advise and help your employees only to make their personal details accessible to friends.

Mark Koek is Lead Expert in Fox-IT's Cybercrime group. He is responsible for Audits, Consulting and Emergency Response.

INFORMATION IS ACCESSIBLE TO ALL

Fox-IT regularly investigates the vulnerability of organisations to 'social engineering'. Social media are an important resource for social engineers. In our investigations, we benefit from using sites like Hyves, LinkedIn and Facebook. Here we collect as much information as possible about employees and their role in the company with which we can target organisations as a test. When we explain our working method at the end, everyone is amazed about how much information is accessible to us all. That realisation is the first step to better security awareness.

FORGOTTEN YOUR PASSWORD?

Exposure to the internet is not the only risk of social networking. What about your clients? If you offer services to private individuals through your website, you probably have a 'forgotten your password?' function on the site. In addition, a 'security question' is often used. American sites like to use the mother's maiden name as a security question. My mother's maiden name is very common, so I don't use sites like these. But even if your mother has a very uncommon maiden name: are you sure it can't be found on your Facebook page? I can assure you that you can find lots of answers to security questions on Facebook, Hyves, LinkedIn and Twitter.

SPREADING VIRUSES

Apart from the social aspects, sites with lots of user interaction are ideal for abusing vulnerabilities like 'Cross-Site Scripting'. Five years ago, a very innovative virus appeared which was only spread through a 'Cross-Site Scripting' leak in MySpace. 10,900 profiles on MySpace still have the tagline "But most of all, Samy is my hero" from this virus. Twitter also encounters problems on a regular basis; the user interaction is obviously huge, so there is always the possibility of a similar problem occurring. Thus far, the viruses have been relatively harmless. However, there is no reason why such viruses could not involve large-scale information collection from 'friends-only' information. Or that a virus could take control of a police force's Twitter account used to provide information to crowds at big events[1].

FACEBOOK ON THE BLACK MARKET

Fraudsters have also discovered the social networking sites. There is now a brisk trade in stolen Facebook accounts. On returning from holiday, an American woman discovered that all her friends thought she had been stranded abroad. Someone had written on her page that her money and tickets had been stolen. Of course, her friends had all sent money to help her. Unfortunately, this money went straight to the fraudster, who had stolen the login data of her PC and Facebook account. Because people have such great faith in social networking sites, this type of fraud is becoming increasingly common. Fox-IT can help you prevent your business network being accessed through the information found on social networks. But the responsibility remains with the employees themselves. ■

[1]The Hollands-Midden police recently experimented with this during the festivities marking Leidens Ontzet

DYNAMIC INFRASTRUCTURE:

Working flexible and secure

In modern organisations, employees want to be able to work anywhere, at any time. Independent of place, time and infrastructure. This is the New World of Working. But what happens when employees have access to classified details and documents? Employees cannot take their secure, fixed workplace with them. In a new dynamic infrastructure, your employees can work flexibly and securely.

Does your organisation handle sensitive or state secret information? If so, you will need strict security measures for documents, data and computers. In practice, this often means working with different networks with their own servers, cabling and workstations. In the worst scenario, an employee will have several computers at his workplace in order to access all the data. This makes it difficult to view data from outside the organisation. Furthermore, it is very time consuming for your system administrator if he has to visit all the workplaces for every maintenance job. There is another way. New technology makes it possible to secure networks and documents, whilst creating a practical and flexible working environment for employees and system administrators. The balance between threat, value of the information and operational use is thereby crucial.

WORKING WITH CONFIDENTIAL DATA ANYWHERE, AT ANY TIME

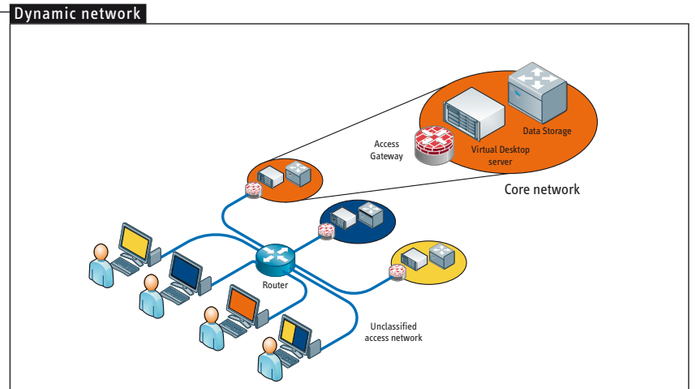
In the New World of Working in a dynamic infrastructure, your employees can access their working environment and documents anywhere and at any time. This was once unthinkable, because of the flexibility versus security dilemma. However, new technologies and improved risk management make this possible. With a few modifications to the ICT environment, your organisation can create a dynamic network which allows your employees to work secure and flexible.

DYNAMIC NETWORK: SECURE AND FLEXIBLE

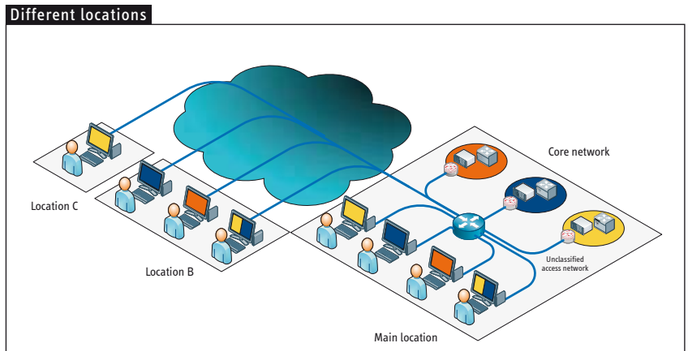
A dynamic network combines high security with the possibility of flexible working. To do this, you use three components: core networks, workstations and an access network.

The structure is actually very simple. Your confidential information is stored on core networks. Each classification level has its own core network. Your employee can access the data through dedicated workstations. To do so, he first creates a secure connection with a gateway which separates the classified and non-classified environments from each other. He then has access to his own virtual desktop on the core network. Through this desktop, he can acces and edit data secure. The connection can be made anywhere: at the office, home and on the move. If an employee breaks the connection, his computer or mobile device contains no more confidential data. And the employee can directly connect with another core network. He can thus work flexible and secure.

Dynamic network



Different locations



TRUST IN YOUR ICT

A new, dynamic ICT infrastructure must naturally be optimally geared to your organisation. Which ICT solution you choose depends among others on the frequency with which classified data are accessed, the threat you wish to protect the data from, the value of the information and the demands or wishes of users. Regardless of the chosen solution, it is important that you can trust the security of the hardware and software you use. Fox-IT is happy to help you consider the options, the threats and the solutions to be applied. For the security of classified information, we often work with the Netherlands National Communications Security Agency (NBV). The NBV provides assurance by extensively testing security products for a certain classification level. Furthermore, the NBV can provide input for the risk analysis related to the use of new solutions.

SUITABLE SOLUTION

Do you need help in designing, developing or implementing ICT which supports the New World of Working? Fox-IT is happy to provide support. We have extensive experience with securing classified and state secret information. Fox-IT develops its own products or looks for reliable products from other suppliers. Furthermore, we work closely with the NBV. In this way we can always offer a solution which suits your organisation. ■

More information? Download the white paper about flexible working with state secret information on www.fox-it.com. Or call Paul Bakker, Manager Crypto & High Security on +31 (0)15 284 79 99 or bakker@fox-it.com

ADVANTAGES OF THE NEW WORLD OF WORKING

Flexible working sounds great, but what are the benefits?

- Higher productivity: the productivity of employees very much depends on the ICT resources at their disposal. If these meet their needs for flexibility and mobility, then your people will work faster and more efficiently.
- Lower administration costs: with a dynamic network, you keep control of the administration costs. Your network is less complex and thus requires less maintenance.
- Better security: sensitive information always stays on the core network. Workstations never contain confidential data.
- Ready for the future: a dynamic network is flexible. You can easily adapt or expand the network if your organisation requires it. For example, by adding extra workplaces and create connections between core networks where necessary.

THE SINA VIRTUAL WORKSTATION is a fully fledged laptop and protects your locally saved data and the communication with your classified networks. The Virtual Workstation is very flexible and makes it possible to run the different classified sessions simultaneously. By using virtualisation in a safe environment, you can continue to work with your normal Windows or Linux environment and still create a safe connection with your SINA network. This can be wired or wireless (UMTS, WiFi), at home, at work or on the move.

SECURE MOBILE WORKING WITH MOBIKEY

With the MobiKEY USB stick in your pocket, you can work on any computer with your own desktop. Plug the MobiKEY into a computer and continue to work. After removing the MobiKEY, no information remains on the computer. The USB stick is therefore ideal for organisations that want to work flexibly with classified information. Various government organisations and financial institutions already work with the MobiKEY.

News items

FOX DATADIODE IN SPECIAL EXERCISES (CEPNIC)

On 2, 3 and 6 September, the CEPNIC exercise took place in Den Helder. This is a joint operation of various armed services. The aim of this exercise was to link the various information systems to create a common information centre: the Joint Common Operational Picture (JCOP). The screen in the JCOP shows various activities of the participating armed services in the operation area. With this overview, better strategic decisions can be taken. In this exercise, two Fox DataDiodes were used. The data diodes linked the various networks with the JCOP through a one-way connection. This guaranteed that the secret information about the armed services could not leave the JCOP or be accessed by hackers.

Events

Expert meeting
'privacy at work and undesired employee behaviour'
Date 30 November 2010 **Speakers** Christian Prickaerts - Fox-IT, Marion Hagenaars - Cordemeyer & Slager / advocaten b.v.
For more information, visit www.fox-it.com

Legal experts

The forensic experts Steffen Moorrees and Christian Prickaerts have been awarded the title 'Legal expert'. After completing an intensive study programme and a research paper, they both passed with a grade 8. This title is important for the continued quality assurance of Fox-IT's forensic investigations. You can be confident that our investigations can be used in criminal lawsuits.

Fox DataDiode NATO secret certification

On 5 October 2010, the Fox DataDiode was approved according to the 'NATO green scheme'. This means that all NATO countries recognise that the Fox DataDiode may be used to process Nato Secret information. The Data Diode connects two networks with different security levels through a one-way connection. This prevents data being sent, publicly or secretly, from the high level secure network to the low level network.

FoxDataDiode
SECURE ONE-WAY COMMUNICATION

TRAINING CALENDAR

Date	Training
1 to 5 november	Hands on Hacking
3 to 5 november	Customised training Investigating on the internet
4 to 5 november	Customised training for SSR
8 to 12 november	CISSP incl. exam on 11 december
15 to 17 november	FoxReplay Basic training for Users
18 to 19 november	Customised training for SSR

Date	Training
22 to 26 november	Investigating on the internet – Basic
29 november	FoxReplay Basic training for Users – Short
30 november	FoxReplay Support training
2 to 3 december	Investigating on the internet – Refresher & in-depth
6 to 8 december	People profiling using open sources