

FOX files

March
2010



Critical
infrastructure
threatened

4

Joined forces
in tackling IT
Paradox

10

The fifth
army

12

BARE BODY SCANNERS IN HAYSTACKS

Or actually body scans at airports. These are placed anywhere these days. Specifically after December 25, 2009. On that day there was a terrorist attack inside an airplane. We can say with pride that the attack was foiled by a countryman. How logical is that? Or should we say: how illogical?

We of Fox-IT, as guards of the digital society, mostly copy the tricks of the physical world, but in this case I look at it the other way round. The security concept that is used in an airport is similar to the traditional way of guarding information: a thick wall around the object that needs to be secured and controlled at all the entrances. In our jargon a fire wall that started as a gate filter, grew to be a 'deep packet inspection' and so on. Whenever there was another attack, the gate controls grew more advanced and more extensive. The virus scanners, malware scanners and Trojan scanners surfaced. The body scan belongs in this picture.

'My advice would be: throw out the supplementary scanners and invest in behavioral analysis'

Two questions arise in this case. Question one: are we secure enough and should we accept the remaining risk? And question two: if you wish to deter new, targeted attacks, what should be the best way to go about that?

For me question one is easy to answer. With the current measures in place no attacks on planes have succeeded after 9/11. Just a handful of attempts have been made in which terrorists managed to get to or even into the plane. Fortunately these attempts have been thwarted. Comparing this to the number of flight movements in the past nine years this question prompts me to saying 'yes'. Especially because attacks on buildings, tunnels or during festivals with the same impact, would be much easier to realize at this moment.

The second question is more difficult to answer. Here too I refer to our area of expertise and I want to make a comparison with cyber espionage. This rapidly increasing form of espionage is really difficult to avoid. Recent examples like the infiltration at the Dalai Lama's computer systems and espionage at Google in China clearly illustrate this. There is no doubt that Google has

a good knowledge of security and still hackers succeed in entering the systems undetected.

The problem of targeted attacks is the enormous advantage that the attacker has because he can invent an unlimited amount of creative possibilities and tests. He only needs to take into account the existing security measures at the gate. Because of the wide variety of traffic that enters the gate, it is an unequal battle which is always won by the attacker.

Digitally the solution has been found in complete monitoring of traffic in combination with real time anomaly detection. Espionage detection has increased drastically with that. In the end the required secret information is meant to reach the attacker. To get there he will behave differently at one point or another. Like the terrorist on his way to the plane. An explosion does not occur by itself. One needs abnormal behavior to set it off. To my knowledge Israel is the only party that subjects all air traffic to complete monitoring. This in combination with real time anomaly detection. The result: up to now there have not been any attacks on planes of a country and people who have quite a few enemies.

My advice would be: throw out the supplementary scanners and invest in behavioral analysis. The digital world teaches the physical world a lesson and it has reached adulthood. A good reason to read about the developments surrounding data diodes, hacking and security model SABSA in this newsletter with another mind set.

Menno van der Marel,
Chief Executive Officer



Menno van der Marel

Colofon

Editorial Board

Joost Bijl
Wendy Groeneveld

Interviews and text

Rijken & Jaarsma, Nieuwerkerk aan den IJssel
Heleen Bongers

Photography

René Wouters, Mijnsheerenland

Design

viervier, Rijswijk

Address

Fox-IT
Olof Palmestraat 6
P.O. box 638
2600 AP DELFT
The Netherlands
T +31 (0)15 2847999
F +31 (0)15 2847990
www.fox-it.com

Critical infrastructure threatened



Try to imagine a malevolent person who penetrates the core of the control panel of a power station. Those who are now envisioning the plot of a modern sci-fi thriller are wrong. Penetration tests have shown weak spots in the networks of various critical infrastructures, whether these are power or water plants, chemical or nuclear installations. There have been documented cases of cyber attacks on critical, digital surroundings. To be able to counter attack, Fox-IT wishes to occupy a more prominent position in the field of security of critical infrastructures. Close cooperation with the various sectors involved needs to be a must.

Fox-IT
Jeffrey Wassenaar
 Coördinator Development
Daniël Niggebrugge
 IT Security Expert

Energy networks and power stations belong to the critical infrastructure of our society. Of course it would be of the utmost importance that unauthorized people would not have access to digital surroundings of power companies. The integrity and trustworthiness of these networks and systems should never be questioned. This requires high demands on the security of the processes involved as well as of the IT. The threat of malevolent people gaining access to the core of these networks is absolutely realistic. Penetration tests have shown weak spots in various SCADA- and 'Process Control' networks. There are known cases of cyber attacks on critical, digital surroundings; national as well as international. The notice that hackers had broken into three American oil companies on various occasions, appeared on January 26, 2010. At least one track leads to China. The hackers were looking for information about the size, value and location of newly discovered oil fields; these fields had not been bid on as yet.

Specific and extraordinary

"When a hacker breaks into a 'normal' computer network, bits and bytes are interchanged and the hacker gains either information or money," tells Daniel Niggebrugge, who works in the business unit of Fox-IT's Forensics, Audits & Training. "A hacker who invades the inner core of a critical infrastructure is able to physically move something. He or she can open a lock or close or open a gas main..."

'Penetration tests have shown weak spots in the networks of various critical infrastructures.'

Jeffrey Wassenaar, Coordinator of Development at the business unit Managed Security Monitoring: "This makes these sectors so specific and extraordinary. The above implies that a clever terrorist does not need to hijack a Boeing to be able to reach his goal. He or she can orchestrate a disaster from behind his or her personal computer."

Joining forces

Fox-IT would like to occupy a more prominent position in the field of security of critical infrastructures to tackle problems like the above-mentioned. To take this responsibility and to tackle the job on hand requires joining forces with all the sectors involved. Jeffrey: "We have noticed that more and more systems have been coupled digitally and this could pose a problem, as many Process Control Networks can not handle this security wise." Daniel: "Because of these couplings, a number of weak links have surfaced in these industrial automation systems. These are systems, which have already been active for years, are used 24/7. Downtime is the worst nightmare in these sectors. And that makes patching these networks or upgrading them very difficult indeed."

No fear

Jeffrey and Daniel do not want to frighten anyone with their message. On the contrary: "Most companies are aware of the fact that new risks have been introduced together with the many links that have been made." Jeffrey: "Those who are responsible within the sectors that we have pointed out, know very well what they are doing. The fact that they are using different networks makes new solutions for security an absolute must. Fox-IT has many ready-made IT-security solutions on hand; these could be implemented easily. For example, the Fox DataDiode. This solution only accepts one-way traffic. Relevant information is distributed, but vice versa is impossible. Non-authorized personnel are never allowed access to critical infrastructures. On the basis of monitoring we can provide insight into possible weak links, or even abort actual attacks within these infrastructures."

SECURE ONE-WAY COMMUNICATION

The Fox DataDiode in practice

The challenge

A European subway company manages an entire subterranean underground network. It has control of two networks: a closed computerized system and a business network.

The closed computerized system controls every subway line. It monitors and sees to it that the signals and switches are functioning. Each subway line within this system is physically and logically separate. Then there is the business network with an information system which enables subway users to view travel information. Management also uses this. For instance to view schedules of working hours of employees and availability of subway car drivers. To provide all parties with exact, accurate information, management has decided to link the computer system with the business network.

‘The Fox DataDiode can never be influenced by logical attacks’

The risks

The Security Officer has performed an extensive risk analysis. It became evident that because of ever increasing professionalization of cyber criminals, it would not be desirable to link the two systems to standard security equipment like firewalls. Systems could be manipulated to cause chaos and do major financial damage to the subway company and its users. The Security Officer is opposed to the management’s wishes because of this security risk.

The solution

The solution to link the two systems was found in a water tight solution, the Fox DataDiode. This solution functions as a one-way proxy which guarantees that information can travel from the subway computer system to the business network, but not vice versa. Through placing the DataDiode between the networks

it is possible to send real-time status subway information to users. This is not done by software, logic or rules, but it is based on physical qualities. That is why the Fox DataDiode can never be influenced by logical attacks; it cannot be programmed wrong by mistake either. This solution satisfies the wishes of the Security Officer.

Fox DataDiode updates

New Fox DataDiode software

- FTP with SSL-support (FTPS)
- Expansion of CIFS with NTLMv2 and (sub)directory support
- Expansion of the password system
- Upgrade of the underlying operating system with support for the latest hardware

Fox DataDiode for Microsoft Windows

There is a new, light version of the software available for Microsoft Windows users. This version offers a lot of flexibility

New features

Windows service Update Server mirroring
Support of mirroring Oracle Databases (based on Oracle Data Guard 11g. Also view www.oracle.com)

For more information about the Fox DataDiode: please contact Bartek Gedrojc via telephone number +31 (0) 15 284 79 99 or e-mail to: gedrojc@fox-it.com

INCLUDING DIGITAL ESPIONAGE IN THE RISK ANALYSIS

Espionage 2.0: the digital threat

Fox-IT
Paul Bakker
Manager Crypto

Espionage seems an outmoded phenomenon. A great inspiration for a thriller, but no longer of this modern age. Certainly not in the Netherlands. What harm could a spy do in this country? But that is not the truth. For years already, the Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (the Secret Service) has been warning about intelligence activities by China and Russia, among others. Holland is an actual target. And not just our government. Our trade and industry as well.

Espionage... A movie or a book does not show how it is really performed. For most information spies do not need to leave the building. Spying can be done digitally these days. Every organization can be reached via the digital highway. A clever informer can gain much, even all the desired information, undetected, should there be a back door in the security of the internet links. Can we arm ourselves against this? Yes, surely. The thing is to weigh the risks and think carefully about the security solutions that could be implemented.

The right mix

The power lies in finding the right mix of regulations, user friendliness and the use of trusted security solutions. Regulations for a certain situation are set from the beginning. User friendliness is measurable and on the basis of commercial information one can find security products that satisfy the need for functionality as well as for user friendliness. But we use the words trusted security solutions for good reason.

Depending on the threat profile of an organization, more aspects than just functionality and user friendliness play a role. Trust in the solution as well as in the producer is just as important. But we should not overlook the confidence in ‘the origin’ of the solution when talking about the security of company or state secrets. In the past, countries have built in back doors in security products to enable them to see what would be going on at a later stage. For this reason it would be prudent for a Dutch organization with a lot of competition from China, for instance, to base its IT-security not on Chinese security solutions. But this holds good for other countries as well!

Trust versus verification

But that is what certification authorities like the Common Criteria or FIPS 140-2 are meant for, aren’t they? Yes, but... the evaluation of a product indicates that it has been basically approved. It is not possible, however, to really verify products. It could be that back doors have been built into versions that do not pass the verifying authorities. And the inside of a chip is very difficult to scrutinize. On the basis of an external specific network packet, the chip can open a back door just like that. So that is the reason why many countries have their own national ‘crypto’ industry for producing really secure products.

So is there nothing we can put our trust in anymore and should we produce everything ourselves? Of course not. That is the good thing about trust. Trust that you can earn. It has everything to do about your situation, the risks, the threats and the organization itself. Put differently: it has to do with the use of reliable solutions that fit your specific situation. The Dutch government, for instance, often uses products from countries with which there are ties of openness, confidence and trust, like Germany and Sweden.

Strong together

Fox-IT is active on a daily basis in the area of security of organizational and state secrets. The trick is to make security reliable and trustworthy. We would like to share our experience in this field to keep the contemporary James Bond away from your door.

Preferably Fox-IT itself manufactures the equipment for the security of state secrets. Fox-IT has developed the RedFox cryptochip in cooperation with the Dutch government. This chip was entirely designed on Dutch soil. The chip is a reliable unit in the security solutions for securing state secrets. The chip can prevent, for instance, that e-mail traffic can be tapped and it can build secure networks.

‘It is a Blue Ocean here, literally as well as figuratively’



In October last year, Fox-IT extended its field of activity in the Caribbean with a branch on Curaçao. After Aruba, this is our second office in this region. Why? Maurice Stolzenbach, Managing Director Fox-IT Caribbean Region, and the man behind our new branch, answers this and other questions. “Doing business is great here and the majority of our market is lying wide open.”

Fox-IT
Maurice Stolzenbach
 Managing Director Fox-IT,
 Caribbean Region

The branch in Waaigat Business Center on Curaçao had hardly opened its doors for a few short months, when a few clients of the Giro Kòrsou bank (GIROBank) saw amounts of money disappear from their bank accounts. This was the job of a gang of hackers that struck, using ATMs abroad. The thefts were soon discovered and the bank contracted Fox-IT. The local newspaper Amigoe wrote: ‘The bank has brought in the well respected, anti-hacker firm Fox-IT in the Netherlands to trace the leak.’ For a branch that is busy getting recognition in the Caribbean, this was superb free publicity.

Manager Maurice Stolzenbach, who forms the management team for the Dutch Caribbean region together with colleague Eric Eekhof, manager of the Aruba branch, which is comprised of four Foxers, says: “This case is great for our familiarity; we have noticed that various well respected parties in this region are taking us seriously after this publication.”

Tackling the problem

The reason for opening a new branch in the Caribbean, has a lot to do with the increase in the demand for Fox-IT’s products and services in the region. This demand has been growing in Curaçao and Bonaire. “These markets were not easily and adequately covered from Aruba,” says Maurice. “Aruba has a separate status and that makes certain things complicated; starting with a simple flight. For several parties, our location proved too large a barrier, but that problem has now been tackled. I am now almost literally around the corner from our clients. They certainly appreciate that.” These clients are specifically based in the financial sector, governmental services and several investigative services.

Maurice: “Our goal is to add various large and socially important parties. For instance public utilities, airlines, hospitals and the telecommunications sectors. We wish to present our image in these sectors in the near future.”

Thinking along

The main difference with the Netherlands is that Fox-IT in the Caribbean is only brought in at the moment when there is a security problem. “We would prefer clients to engage us in their IT-processes in an early stage. In Holland, that is often the case. This puts us in a position that enables us to become involved in security and implementation of the ICT surroundings. In this way



Fox-IT opens office at Curacao

we can prevent security problems. Besides recruiting new clients and gaining improved familiarity, there is another important aspect to our presence here: we wish to be involved in trajectories at an earlier date, not only to react to incidents.”

Blue Ocean

“We offer a lot of extras in addition to the local knowledge and work closely with the local companies. We develop solutions for the protection of state secrets, conduct digital forensics investigations and deliver security expertise in the form of audits, managed security services, consultancy and training courses. We carry out special projects in environments where security is vital. In that way it’s a blue ocean here as well. Literally as well as figuratively. It is nice doing business with the people here and the market is largely wide open. Moreover, it’s a good place to be. The temperature is not a day under 28 degrees, the water is bright blue and the beaches are bright white...”



FOX-IT AND PINK ELEPHANT JOIN FORCES IN TACKLING IT PARADOX

SABSA: organize security with a mature methodology

Fox-IT
Eward Driehuis
Manager Works

During this tough, economic time a few very well-respected financial institutions and organizations have overlooked certain risks. For some this meant a final goodbye, others survived thanks to the support from the government. Painful instances are known in other sectors as well. Think about the secret governmental information and patient information that were there for everyone to see... Despite sizeable investments in TOGAF, ISO 27000, COCO, COBIT, M_o_R and other frameworks. Despite regular internal and external audits. Despite all the energy that has been put into it. Clearly the current approach of enterprise risk management is not enough. Because the current approach holds strong, but also weak points. Some applications are targeting a specific part of enterprise security; others focus totally on the approach, the 'what', but they forget 'the how'. In actual practice we regularly see that (undetected) white spots occur when combined applications are implemented. More often than once, these spots might be the cause of unpleasant surprises.



SABSA

In this perspective we might like to draw your attention to SABSA, the Sherwood Applied Business Security Architecture. This is a public domain methodology for the development of an organization-wide security architecture.

What makes this method so unique

- Complete: SABSA offers frameworks, models, methods and processes
- Supportive: supports the entire cycle: from design to operation
- Scale: from an isolated project to a complete organization
- Public domain: free use, complete independency of supplier
- Protective: protects your investments, does not compete with, but entirely connects existing frameworks
- Guiding: guides (business) management effectively towards acceptable risks for the organization
- Connecting: SABSA closes the gap between business and IT

Why SABSA?

SABSA enables organizations to connect company goals, security, ICT and organization. Good security starts with the phrasing of the question what should exactly be guarded on a business level, why, how, by whom and when. The answers to these questions are then translated into a security architecture, after which the technical solutions are implemented. Operational management normally runs parallel to this. In the case of lack of grip this rapidly becomes complex and poorly organized. The strength of SABSA is that it divides this complex territory into well-organized and structured layers. Moreover, it helps fill in the details, so that the big picture remains clear. This prevents that white spots or isolated security solutions occur. SABSA also makes the security architecture measurable and visual. A CISO can show his CEO the state of affairs at any given moment and where certain areas of attention are located. Just as a business manager has insight at any given time how his or her business assets are protected.

On the other side it becomes visible what use the various implemented solutions – and resulting costs – have. This dual traceability time saves time-consuming and ever returning discussions and obscurities. Besides, it makes the organization auditable.

Cooperation Fox-IT and Pink Elephant

Fox-IT is joining forces with Pink Elephant. Fox-IT has the best technological knowledge and experience to design security solutions at the highest level in difficult situations. Pink Elephant leads the way in IT-Service management. Pink Elephant introduced the service management methodology ITIL in Holland in the '90s. This method has become the market standard through the years.

Rene Bosselaar, director of Pink Elephant: "Business and IT cannot be viewed separate from each other anymore. Almost daily we read in the newspaper how malevolent persons are using the same IT to harm organizations. I therefore speak of the IT-paradox: IT is a business enabler 'pur sang', but at the same time it is the largest threat for your company's continued existence. Pink thinks therefore that it is necessary that security will become an integral part of the service strategy- and design processes of Service Management. In our search for a robust approach, SABSA distinguished itself at essential points: the business is the point of departure. Contrary to many other approaches, this method is not fragmented to boot."

Eward Driehuis, Manager Fox Works: "Too often we see security measures that have been based on happenstance, intuition or emotions. There is only one thing important: the goal of the organization. The rest is just a derivate. Good ICT-guards are needed to make the grade. SABSA is a terrific aid with that."

'SABSA makes the security architecture measurable and visual'

Tackling the IT-paradox together

It is therefore logical that Fox-IT and Pink have joined forces. Both parties go around together visiting clients and helping them with sound advice and on-hand service in solving the IT paradox.

More information about SABSA and ICT security management? Please get into contact with Eward Driehuis: +31 (0) 15 284 79 99 or driehuis@fox-it.com.

ATTACKS AND ESPIONAGE VIA THE DIGITAL HIGHWAY

The Fifth Army

The sovereignty of the Netherlands has been guarded for ages by the Ministry of Defense. The four divisions of our armed forces guard Dutch territory and assist with operations abroad. But the world is constantly changing. Through the increasing technological developments and dependency on ICT, countries are more vulnerable than ever. Company networks and our vital infrastructure could not function without access to the internet. Frequently stories about attacks and espionage via the digital highway surface on the news. In 2007 Russia initiated a large-scale cyber attack on Estonia, where governmental organizations, media and financial institutions were targeted. In 2008 it was Georgia's turn. It is understandable therefore, that lack of policy and a budget for cyber warfare in the Defense Budget for 2010 led to questions in Parliament last December, 2009.

Outside the Netherlands, there have been several countries that have installed a cyber army. The United States, Great Britain and Germany, among others, have a special unit focusing on the digital scene of action. Why is there no such thing in the Netherlands? Already in February 2000 questions have been raised in Parliament about Dutch developments regarding cyber warfare as a result of a television episode of 'Netwerk'.

Lacking Frontiers

But what is the big difference between the digital and traditional scene of battle? In the traditional way of waging war, our frontiers are clearly defined. Should a large army appear on the radar across from our borders, we receive a warning of a possible attack. Attacks from further away are even easier to detect.

In cyber warfare this is much more nontransparent. Through internet the Netherlands border on all the

countries in the world. Digital traffic travels 'with the speed of light', 299,792,458 meter per second, to be precise. This makes foreseeing an attack before it has reached our digital borders, almost impossible. And then we assume that we can indicate our digital frontiers. That is not so simple at all. Although most internet traffic enters our country via a few intersections, it would not suffice to determine these as our digital border region. The possibilities and structure of the digital world allow a person with a satellite receiver to link our digital infrastructure anywhere in the Netherlands with the rest of the world.

Cyber Defense

From the above one may conclude that prevention at digital borders is a hopeless task. But detection against it is essential at the major intersections in the Netherlands. Therefore we should see to it that all the important networks have been secured individually.

Back to the castles of yesteryear, it seems, but then with a clever, central, detection network. Because just detection and prevention at the important networks would not suffice.

Common Operational Picture

For a reliable Cyber Defense a Common Operational Picture is needed of our digital world. A Common Operational Picture allows an overview for the commanders, so that they can react adequately. A battle field? Yes, for sure. Dutch digital infrastructures are attacked from abroad on a daily basis. The two previous annual reports of the AIVD clearly point to this: "In 2007 and 2008 concrete threats came to light of digital attacks on computer networks of the government and the trade and industry in Holland, orchestrated from China." The reality of the threat from China has come to light especially during the past month. Google and more than twenty other large firms in the US have structurally been attacked by China with gaining information as its goal. Admittedly, the goal is at this point gaining information. But these same techniques are used with actual cyber attacks.

Structure

The basis for Cyber Defense is formed by a digital Common Operational Picture. For this we shall need to put in place a structure where large-scale digital attacks can be centrally detected and analyzed. On the basis of this analysis the reaction to this attack may be determined. In a reserved way, defensive or hitting back hard? As to that last option: the digital battle field is a lot more complex than the traditional one. In the physical world one can easily recognize where an attack is coming from. When every minute a mortar is fired from a certain location, the analysis for a counter attack is made easily and relatively quickly. Of course one should take 'collateral damage' into account, but this is something that can be dealt with.

CONTINUE ON PAGE 14 >

'Dutch digital infrastructures are attacked from abroad on a daily basis'



Paul Bakker

Fox-IT

Paul Bakker

Manager Crypto

CONTINUATION FROM PAGE 13 >

Counter Attack

In the digital battle field everything is much more complex. Through the ease with which traffic on the internet may be diverted, it is not possible or hardly possible to determine where the attack has initiated from. An attack that seems to come from a network in Spain may have started in Russia. To stop the attack it is of course possible to counter attack. But although 'collateral damage' can be assessed initially in the physical world, this is difficult to oversee on the digital battle field. A fierce counter attack may result in vital infrastructures in Spain breaking down. Not something to be happy about.

Two Components

Just as with traditional warfare, Cyber Warfare is made up of two components: Cyber Defense and Cyber Offense. The first one deals with the capacity to defend our country against attacks from abroad. With Cyber Offense it is easier to assess the 'collateral damage' than with defense. With Cyber Offense one determines what the target is in advance and what we wish to accomplish there. Surveying the results of such an attack would be easier. But we are not that far advanced in the Netherlands. For this the knowledge and ability should be present. Therefore it is necessary to invest in this, so that that knowledge and ability would be present when we need them.

**'With a bit of luck we may soon be guarded by a fifth army:
the Royal Cyber Force'**

In the fields of Cyber Defense and Cyber Offense, the Netherlands has a long way to go. And while Cyber Offence capacities are still under discussion, Cyber Defense has become an indispensable part of the task of our Government. Through the increasing threat in the digital world the safety of our society depends on it.

Fifth Army?

Although it might not be obvious, the Dutch government is not sitting still in this field. In 2008 the interdepartmental project 'Verkenningen – Houvast voor de krijgsmacht van 2020' (Surveys – a grip for the armed forces of 2020) started. One of the sectors within this project deals specifically with the matter of digital safety. The project's goal is to determine the policy options and resulting budgets for our Dutch armed forces to be prepared for the situation in ten years' time. With a bit of luck we may soon be guarded by a fifth army: the Royal Cyber Force.

Fox-IT – for a more secure society

Governmental organizations, multinationals and other corporate entities trust in Fox-IT for the protection of their highly sensitive information and critical processes. To achieve this we make use of governmental certified security products, experienced security professionals, ethical hackers and IT-forensic experts to name but a few. Furthermore, all Fox-IT employees have been screened by the Dutch intelligence service (AIVD) to handle secrets. All of our services and products are geared towards working with and protecting your secrets. Our mission is "a more secure society".

Cybercrime & Fraud Services

Penetration tests for security testing on networks, applications and source code by IT-security experts with a hacker mindset. This process immediately exposes your risks allowing you to take the correct actions in order to improve your information security level.

FoxTeam tests the entire security process within your company without the normal limitations. This is achieved through so called "ethical hacking", exposing the weakest link in your security network.

Passive Audit (PA) judges the function of security measures in your network based on an analysis of actual network traffic during a predefined period of time. Because of the passive nature by which the data is collected your network infrastructure is not affected or disrupted by the process. PA offers a unique insight into what happens daily within your corporate network.

Managed Security Monitoring (MSM) offers 24x7 real time, high quality monitoring, analysis and incident response services for securing your network, applications and data in the fight against cybercrime. As a trusted 3rd party, Fox-IT continuously guards your infrastructure in order to identify anomalies and allow for the proper response.

Emergency Security Monitoring (ESM) offers a 24x7 increase of the security level of your vital networks, during a limited period of time during which your company may be experiencing a heightened security risk. ESM is a short term application of MSM

Transaction monitoring for online banking (DetACT)

offers 24x7 real-time, high quality monitoring, analysis and incident response services for securing online transactions, specifically focused at online banking. Swift detection of malicious online transactions which results in the possibility to identify and prevent online fraud. DetACT assists in quick and high quality fraud investigations by providing direct and complete transaction information.

Anti Fraud Services continually investigates and monitors online transaction channels of financial institutions in order to identify any and all threats. You are always aware of the relevant attacks on your online transaction channels allow adequate and timely prevention measures.

IT-Forensics conducts digital investigations and data recovery by leading IT forensic experts. Digital evidence is retrieved, secured, processed and investigated according to the correct forensic methodology, allowing results to be used as evidence in a court of law. Fox-IT is a recognized private investigation firm.

CONTINUE ON PAGE 16 >

Intelligence Solutions

FoxReplay Analyst is a product which allows the reconstruction of intercepted internet traffic to such a format that it is easily available, understood and analyzed by anybody. Thus no longer limiting this process to specially trained individuals.

Crypto & High Security Solutions

Fox DataDiode connects two networks with varying security classifications by means of a secure one way connection. This prevents that data is, intentionally or unintentionally, sent from a highly classified network to a less classified network. For the Fox DataDiode there are a number of applications available such as (but not limited to) FTP, Windows File sharing, Database Mirroring, Antivirus updates, Microsoft updates and SCADA protocols. The Fox DataDiode is approved for connection of networks up to and including NATO Secret and is a Common Criteria EAL 4+ certified product.

RedFox Cryptochip is the basis for the next generation of products intended for the protection of state secrets. Making use of Dutch cryptography products for the protection of state secrets.

VPN for secure connections between various networks, including those containing classified information (SINA product line is approved up to NATO Secret). For the commercial market there is a choice of a number of products including our own version of OpenVPN. Secure connection of networks without effecting the reliability or integrity of your network.

Secure teleworking solutions, for classified information as well (SINA Thin Client). For the commercial market the offerings are G/On and OpenVPN products such as "VPN-on-a-Stick" amongst others. Secure teleworking without affecting the reliability or integrity of your network.

Secure workstation specifically for working with highly classified information. Ease of use is improved by combination of classified and unclassified workstations in a safe manner. Thus allowing one to work on both classified and non-classified information from a single location.

Data-at-rest encryption encrypts data either through a software or hardware solution. Examples are Safeguard, Decru, or our in-house developed RedFox Disk Encryptor. In the event of theft, loss or damage of storage media one can be assured that only the appliance has been lost, not the data.

Secure Telephony Solutions through encrypted phone connections that cannot be intercepted. Our solutions are approved for National sensitive information (VECOM/Sectra Tigers) or for commercial secrets (SecuVoice). Have secure conversations that cannot be intercepted as is possible with the current GSM and DECT network.

Special projects in an environment where exceptional security is vital. Results are often a combination of standard IT products with limited customization, resulting in creative and effective solutions that are easily implemented without compromising your security demands.

Security Consultancy & Training

Consultancy by IT security experts. Fox consultancy is not only a knowledge injection into your organization, but also the assurance that security demands will get the correct attention.

Outsourcing of screened IT security professionals, ICT security architects, Information security officers or Forensic readiness experts. Unique expertise that is directly available to you and your organization or classified project team.

Training by our experts in such fields as Online Investigations, CISSP, Hands-on-Hacking, and Secure Coding as well as tailor-made security courses increase the security knowledge in a practical manner that can be implemented immediately within your organization.