varnostni forum

KORAK PRED VARNOSTJO
www.varnostniforum.com

11
Letnik V / 2009

TEMA MESECA:
RAČUNALNIŠKA IN MOBILNA FORENZIKA

HELENA DVORŠAK
Detektiv in forenzika IKT

MATEJ SAKSIDA
Pravno-formalni vidik forenzičnega zasega podatkov

FORUM MESECA:

BOŠTJAN KEŽMAH
Standardi revidiranja informacijskih sistemov

INTERVJU MESECA:
Saša Aksentijević
ICT forensics expert

SAŠA AKSENTIJEVIĆ

ICT FORENSICS EXPERT

Mr. Sasa spent his entire educational and professional life in ICT area. First he worked several years as an independent ICT consultant, an owner of a start-up company and a specialist for mass storage technologies. During the past six years he has been working in one the world's biggest multinational companies in the oil and gas sector which performs offshore and onshore turnkey projects. Several years ago he has decided to continue his formal education. In fact, he is by profession an economist specialized in business informatics, so it made sense to enrol in a master's course in ICT Management and to become also an ISO 27001:2005 Lead Auditor. He also started studying ICT forensics in order to expand his consultancy knowledge base. Now he is a certified court expert.

Now you work as forensic investigator nominated by Croatian court of law and as ICT security manager/CSO/consultant. What exactly do these titles mean?

I have spent pretty much my entire educational and professional life in ICT area. First I worked several years as an independent ICT consultant, an owner of a start-up company and a specialist for mass storage technologies. However, I am an economist by profession, specialized in business informatics. During the past six years I have been working in one the world's biggest multinational companies in the oil and gas sector which performs offshore and onshore turnkey projects. First I worked as system administrator for a short period, than I was responsible for the ICT department. With years passing by I gathered experience and due to the business requirements, the board nominated me to a position of an Information Systems Security Officer. There I participated in starting with implementation of systematic ISMS in the company. Finally, a few years ago I have been also nominated to a position in one slightly different area – health and safety, where I hold a post of a president the a steering committee in charge of implementing company's health and safety strategy. When you combine ICT security and HSE, you pretty much get to a certain point where you have to deal with security as a whole and not only with information safety or safety at work.

Several years ago I have decided to continue my formal education. In fact, I am by profession an economist specialized in business informatics, so it made sense to enrol in a master's course in ICT Management and to become also an ISO 27001:2005 Lead Auditor. However, I consider myself to be more of a generalist than a specialist, so I have also started studying ICT forensics in order to become certified court expert and to expand my consultancy knowledge base. I am professionally interested in large organizations and plan to start PhD studies in business economy, but I am still looking how to incorporate integral security, forensic models and strategic ICT into this field.

How do these two things forensics and security consultancy combine? Do you think is necessary to be an ITC security consultant to be a good forensics investigator?

In most organizations whose information security systems I had an opportunity to get to know I have noticed that ICT security is primarily considered a technical discipline. This means that even the top management believes that information security is primarily an ICT process that can be achieved just by investing in hardware and software. Furthermore, many people think that incident recovery and business continuity are also among responsibilities of ICT. I have always strongly opposed such opinions – my personal experience is that security and continuity goals can be achieved only through synergy of all organizational units and raising awareness and training of all employees, as well as through setting up logical, simple and best-practice oriented procedures.

In order to be a successful forensics investigator it is important to have significant amount of experience working not only as forensics expert, but also in the general area. I have started working very young at the very beginning of my university studies, so by now I have gathered 18 years of working experience in the area of ICT.

Understanding technical context is only a part of the whole story. Forensics expert usually has to work with people as well, not only with information systems and hardware. He also has to engage large and complex systems like courts and corporations. So, it helps a lot to have good understanding of business framework, corporate culture and to have legal knowledge. Many people fail because they have good technical knowledge but they cannot clearly express professional opinion. Having the knowledge of ICT security is certainly a prerequisite to be successful in this job, but it is even more important to have the ability to deliver reproducible results that can be passed on to the judge. I always like to say that successful forensics investigator should be able to produce results that can be understood by people who are not in the field and that the report he delivers should not be longer than two pages no matter how complex the case may be.

How did you become a forensic investigator? How many years do you work in forensics?

In Croatia court forensics is regulated by a special law. The institution in charge of training of new forensics experts is Croatian Association of Court Experts. Training of new candidates consists of theoretical and practical part. The practical part is executed under mentorship of a mentor who has been working in this area for years. The candidate has to fulfil strict selection criteria and has to produce at least five real cases to be presented to the court. After that, the mentor presents a report to the Association stating who he would recommend as a candidate for a nomination to the court. Other preconditions for nomination are health certificate and professional liability insurance policy. I am nominated at two courts: the commercial court and municipal court. This means that I can cover all cases, from criminal to private law suits and I am also authorized to provide third-party consulting and make forensics reports for private clients. My formal liaison with forensics field is relatively fresh and spans for the past four years.

How does your typical work day look like?

You can imagine that doing several jobs is not an easy task so everything has to be well organized. Of course, nowadays multitasking is a must and I do not think there are many people that enjoy the benefit of doing one thing at a time. Considering that I work full time in my company, I pretty much use all my "free-time" to get additional education, work with clients, participate as a lecturer at conferences and write articles. I am lucky that I work near all the courts where I am nominated and in the centre of the city so I can quickly get in touch with people and get information. Of course, Internet

helps a lot, but sometimes it is very important to interview people personally and get first-hand impressions and evidence for the cases.

Which forensic hardware and software do you use?

There are specialized forensics investigation suites on the market that are in the ICT forensics investigations often referred to as a golden standard. Every forensics investigator has a set of his own tools that he uses for various purposes, and usually collects these tools over the. I think that tools are not important, the results are important. Big name cannot make up for sloppy investigation process. Forensics should provide clear cut answers using scientific method that can be easily reproduced – it is not important that the tools used to get the results have big names.

However, there are great tools available that are in fact collections of open-source software that work on a very low-level and can be used for analysis. Also I like some ethical hacking tools that I have come across and incorporated into my arsenal of forensic utilities.

Do you also work in GSM / PDA forensics?

I might be able to provide such services and have the necessary knowledge as I am a nominated forensics expert for informatics and telecommunication systems, but until now I have had just one case that involved mobile telephony forensics directly. However, I would not distinguish between GSM/PDA and computers anymore as they are heavily interconnected and run operating systems so there is no clear difference between telephony and desktop computing anymore. Take for example PDA vs. net book with SIM card slot. Both run operating system, both are used primarily for remote data processing, the only difference is the format!

What practical experience in the field of forensics you have?

First of all, working in ICT security field inherently forces you to work sometimes as an investigator. Often you need to deal with security breaches, with techniques to mitigate risks or to find out what went wrong and who did it, even if it is informal. If you are working in a big system, you will spend a significant part of your working time trying to get to the root of various security issues. These things are not to be taken easily and it is my opinion that people who have good experience in this field are good candidates for forensic experts.

Very often people require expert's opinions when they need to decide by themselves or together with their legal representative how to proceed with certain court cases or disputes that they are involved in. Court expert's opinions can be used as a basis on which it is possible to set directions how to deal with the case. The opinion of the court expert can be submitted in form of "other opinion" or "other proof" that the court can also take into consideration. Even if the opinion is not presented in court, it can give important guidelines what might happen in the court of law and whether it would be beneficial for the party involved to go into certain direction.

The third area is direct cooperation with courts that assign a case to the forensics expert asking him for a clear opinion on certain matters.

Can you tell us yours major achievements? What was the biggest forensics case you solved?

Of course, I cannot disclose any details, but almost every case a forensics investigator deals with is very important, as it involves potential financial impact, prison penalty or other implications, like loss of a job. There are no "small" cases, just cases with lower absolute impact. It is always nice to see that a dilemma is resolved or that a clear answer is given to a question that was crucial in order to solve a case or that to explain something which was a bit unclear.

What were the biggest mistakes made by other forensics that you have come across as an advisor to the court?

Court experts should be able to formulate their findings clearly without using too many technical terms, as their opinions will be used by people who are not experts in this area, for example lawyers, judges and managers. Therefore, forensics experts should refrain themselves from using long and too technical explanations. They should know how the legal system works and which its requirements are. This means that every expert's opinion must be completely objective, must be supported by evidence and must be reproducible under the same conditions. Forensics experts must refrain from any subjectivism in their findings and there is absolutely no place for guessing.

Systems are so complex nowadays that sometimes one single court expert cannot do the work himself and has to call for help colleagues or professional institutions. Accepting too much work is something that is likely to lead to people making mistakes. Also, judges sometimes complain to me that some experts are not punctual in their work. The judge will assign a case asking for results within 30 days which is quite reasonable time, while the expert will accept the case and will not be heard from for the next 6 or 8 months, during which the trial is on a standby. How can such an irresponsible expert be taken seriously?

Last but not least, the forensics experts should be independent, professional in approach and honest in their findings and when expressing limitations.

In the future of forensics what do you think the greatest challenge and the limitations will be?

If cloud computing will be the next "big thing" in the development of ICT systems, it will be interesting to see how computer forensics will address challenges brought along with distributed computing. No current formal system or model of information security is able to adequately address the information security in a structural way and consequently to easily trace activities in a cloud computing environment as the traceability depends primarily on voluntary involvement of pathway components. Development of communications will bring along also forensic investigations of GPS systems – it is just that forensics cases are usually a bit late as they tend to follow up the introduction of technology.

Also, a lot of information that experts need to form an opinion about is kept within regulated systems that are not public (ISPs, government services), so it will be interesting to witness the direction this regulation will take in the future. Currently, there is a trend of a strong regulation and centralization that I endorse from the viewpoint of a professional in ICT forensics but strongly dislike from the point of view of human freedom.

Do you have any advice for colleges and others related to forensics and security?

In forensic investigations, it is very important to define the exact scope of investigation that has to be agreed with the judge or the client who asked for the expert's opinion. It is not possible to produce clear answers if the question is not clearly formulated.

Experts are often under pressure to produce quick results but sometimes they tend to forget the basics. The original evidence must never be contaminated in any way as the findings can be then disputed. The actual investigation is never done on the live evidence, but on digital copies.

Finally, many ICT security projects fail because they did not have a sponsor in the very beginning. Unless ICT security is endorsed by top management or some other top level sponsor, it will probably bring unsatisfactory results. So, social networking is often an overlooked part of the overall ICT security scheme. *

Spraševala: Tanja Grdina