

Varnostni forum

KORAK PRED VARNOSTJO
www.varnostniforum.com

10
Letnik V / 2009

FORUM MESECA:

MATEJ SAKSIDA
Socialne mreže
kot orodje za
preverjanje ozadja
kandidatov za
zaposlitev

IVAN KOBAL
Varnost informacij
v perifernih
informacijskih
sistemih bank
in hranilnic ter
drugih finančnih
organizacijah

INTERVJU:

Gunnar Porada

Misunderstanding of IT-Security makes hacking easier than ever

TEMA MESECA: INFOSEK

JANJA JEDLOVČNIK
Implementacija in kontrola notranjih
pravil za e-hrambo – primer iz prakse
v večji banki

DAMJAN NOVAK
Zunanji varnostni pregled – zakaj in
kako!

JAN ŽORŽ
Ali je „neviden“ IPv6 promet lahko
nevaren za poslovna omrežja?

KJELL KALMELID
The ENISA Awareness Raising
Community





**MISUNDERSTANDING OF IT-
SECURITY MAKES HACKING EASIER
THAN EVER**

GUNNAR PORADA is known as an ex hacker, now a Senior IT-Security Consultant in Germany and Switzerland. He was about 14 years old when he heard for the first time that it was possible to make phone calls for free ... Now his mission is to help companies to fight against criminal hackers. He also helps to raise public awareness and helps people to understand that passports, for example, can be tampered with, the online-banking accounts can be hacked etc. He explains his audience how hacking works and how they can protect themselves against it. Most of the time he has to fight against the misunderstanding of IT-Security and ignorance of the victims.

You have started as a hacker when you were a teenager. Why? What was the reason? Was it just passion, curiosity or something else?

Well, I was about 14 years old (now I am 35) when I heard for the first time that it was possible to make phone calls for free. I was not sure if this was a myth or reality but the idea fascinated me. I remember I was sitting by the phone, picked it up and thought "Now I have to pay for it". I put the phone back down and was sure that this didn't cost anything but I could not make a phone call then. A couple of month later, some schoolmates gave me the frequencies to make Blue Boxing over Chile and I was able to phone for free. But the question remained: Why is it possible? I started to read and learn a lot about it and I have realized that the reason for "the free phone calls" were only bugs in the computer of the phone companies. To be honest – bugs in design. And my very next question was: if those computers have bugs that allow such things, how does other computer look like?

How did you learn about hacking? Was it difficult? Where did you hacked in or for what you used hacking?

Hacking is quite simple – much more than security. You have a target that you would like to reach and plenty of possibilities to do it. You can do it by using technology or just through social engineering. However the more you know about technology the more successful you get. Today Internet makes it even easier to find all the information you need and of good quality. It only takes a lot of your time.

Was it dangerous for you? Did you have any problems with the authorities (for example police)?

Indeed, it was dangerous for me but not because of police. I am not a so called "state-approved-hacker" because in that time the law didn't even consider hacking as a possible offence. I remember some TV-shows where people were discussing whether hackers existed or it was something else behind the incidents? People didn't believe that hacking was possible – but it was and we were laughing in front of TV when we saw it. But it was dangerous for me because for another reason. Many criminal organizations where already very active in this

field and were trying to recruit some guys or were just buying the hacked information.

When did you change sides from hacking to protecting computers and networks? Why?

Something went wrong with a 20 million dollar bank proof check when I was around 18 and I was sure that there were some people very angry with me. I told my mom "It could be that I might have to hide for a while. Don't worry. All will be OK and I will get in contact with you" – I was afraid, afraid for my life!

She looked at me and said "Boy, whatever you are doing with your computer – give it up". And she was right. I started to think about how my life should go on. Should I work for criminal organizations and be happy every day just to wake up alive? Some hackers chose this way because they got addicted to the thought of fast and easy money. But I have decided to sleep at night and be able to look myself in the mirror. The alternative option was a job that a friend of mine told me about. He told me he would start working for the secret service in his country and do "legal" hacking for them.

After a long discussion about how he would apply therefore the job, I realized that his father worked for them, but he died while performing his duties! My very next question to him was direct: "Are you stupid enough to make the same mistake as your father?" He answered me with a very interesting point: "Computer-hacking is passive and not like normal espionage (which is active), even with the same result". I realized that computer hacking changed so many old presumptions we had. And then he said "I will start to learn German, too". I asked him why and he answered me, because my future employers will be German companies...

Since that day it was clear to me that my future career would be helping companies against hackers and espionage! The friendship with this guy ended soon afterwards with words: "Gunnar, go and set up secure environments and I will go and hack them, but we both will have enough to do for our entire lives."

As mentioned now you are Senior IT-Security Consultant. What are now your priorities, duties or better said what is your mission?

The mission I have is to help the companies fighting against criminal hackers. After I have seen the other side and have decided that this it is not the world in which I would like to live in, the logical conclusion for me was to help others to protect themselves. But to be honest – most of the time I have to fight against the misunderstanding of IT-Security and ignorance of the victims. There were many occasions (especially in the beginning) where I didn't even have the chance to help people protect themselves against hackers. I got fired from a bank after I successfully finished my legal hacking job for them. I found a way to hack any of their Stock-Exchange accounts and reported about it to the IT-manager of the bank who ordered this controlled attack. This information was sent directly to the board of the bank and then several discussions followed. A little later they cancelled my consulting project. My impression is that most of the companies just like to get security reports as an alibi like "Yes, we did a IT-Security research and we are safe". No one likes to hear that they are not safe even when they are. The result is like a big bubble that grows every day.

Do you believe that being a hacker helped you to become an expert in IT security? In which way?

Not necessarily but I have realized there is a big difference. A hacker learns to focus on his target. Like an information that is worth something or data that should be manipulated with etc. Normal security experts didn't know about these underlying business values and they focused more on the security mechanisms themselves (Firewall, VPN, PKI etc). By focusing only on the technology you get some (or plenty) large security applications here and there but they are not linked together in terms of the process flow of the company. In this case the hacker just needs to stand like a fisherman on the river bank and wait until the fish bites. And they often do! An Ex- or White-Hacker thinks differently and in a more complex way about security. They combine business values with technology.

Is it possible to hack without any traces? If so, how should we protect our self's and the company?

I am sorry to say it but yes, it is possible. If you're enough of an expert you can delete all your traces in most of the situations. But the most dangerous part is the fact that it doesn't even matter. Even if you leave plenty of traces, nobody notices them most of the time. I saw companies

that used compromised systems for couple of years without realizing it. And they had plenty of possibilities. An Airport CTO told me "We should not scan the internal server" because they knew that majority of the internal servers were "perforated by hackers" and it was better to leave them as they were as long as nobody else realized that there was something wrong.

What in your opinion are now the most critical factors related to IT security?

We have to learn that computer works differently. When data is stolen most of the people still think about it in terms of a physical action - but with computers it is different because you can clone data without any losses. A fact is that a lot of people can more easily imagine that data can be stolen if stored on a USB-stick because it's a tangible object. But over 70% of all web applications are vulnerable by SQL-Injections and no one needs to actually physically enter your computer to steal the entire database - you can do it from the Caribbean beach with a cocktail in your hand. Computers are still something new after being on the market for around 20 years and most of the people don't understand what can be done with them - especially in companies.

Who should be aware? Who are the hackers today? What is your advice to the companies in order to be safe from hacking?

Anyone should be aware because hackers don't make difference among their victims. They hack anyone from physical person to companies and governments and critical infrastructures like power plants, public transport systems etc. The reasons for attacking certain victim might be different. A physical person for example and local companies - like craftsman or supermarkets etc. - could be hacked in order to use their identity and relay their computers in a botnet to make money. Additionally a hacker would try to get their passwords for entering websites, to gain remote access, interfere with e-banking etc. A hacker can steal data from large companies and government to sell it to someone else - competitors, other countries or whoever pays for it. I have already got requests from head-hunters for example, just to steal some additional information about employees in return for money. (Of course I did not do it...) The interests are wide spread and the market for illegal data is vast.

Can you tell us about yours major achievements?

No, it's under NDA, but as you can see in my speeches - beside the fact that I help companies I also raise people's awareness and help them to understand that for example passports can be manipulated, the online-banking accounts can be hacked etc. I explain them how it works and how they can protect themselves against it. By this, I try to minimize another major risk of computer hacking: you can easily become an innocent victim and find yourself in front of the judge to whom you have to explain that a virus or a hacker committed the crime, not you. Hackers use your identity and your environment to remain undiscovered.

How can we learn hacking? What do you suggest ☺?

I don't know and it's really not my intention to teach people how to hack. If you like to help us in the fight against hackers, you have to learn how they act and about the possibilities that are available to them. This is very complex and sometimes it is hard to understand all the different layers, protocols, encryptions etc. behind the buzzwords and marketing bubbles of new products and solutions. But after a while you will understand that security is a process and you have to do it day by day, year by year. You will never be completely safe, because that is impossible. But you can lower your risk and the probability to become a victim by applying any single security solution. Just keep in mind to connect it to your business process. *

Spraševala: Tanja Grdina

