Top priority Security: Quickly transfer a million

The methods of cyber criminals are becoming ever more refined, and they also bring them many millions. "Fake President" requests, disguised invoicing mails or extortion through data encryption caused a stir most recently. How to protect yourself?

Whether brutal or clever, fast or well-thought-out, cyber-crooks are continually developing new methods that are worthwhile for them in any case. Up to 500 billion euros, the dark deeds are supposed to cost the world a year. From the good old Denial-of-Service attacks, where the company IT is flooded with inquiries and paralyzed with brutal computing power - usually by previously captured PCs and servers - if a good protection is not paid honest, for example via so-called Ransomware, these are small, fine malicious programs that encrypt all company data, right up to the true masterpieces of the cyber crimes, where the really large amounts are collected by diligent and patient spying and sensitive personal support. This includes the "Fake President Fraud", particularly embarrassing for financial departments. The FACC AG, based in Upper Austria, cost about 50 million euros - and the financial director the job.

50 million away

The criminals, with this clever method, are so familiar with the company and the key executives, that they finally convince financial accounting at the right moment to transfer large amounts to fake accounts (for example, for a secret takeover). In the case of the FACC, "only" FACC Operations GmbH was affected, while the IT infrastructure, data security, IP rights as well as the operational areas of the company were spared from the criminal activities, according to a report. How the million coup was running is still unknown. At present, investigation is still going on and any claims for damages and insurance claims are examined. But beware: Insurances do not pay for negligence!

"The method to mimick/impersonate the boss is certainly the most impudent one and works very well with internationally operating companies," says Dieter Steiner, CEO of the German cloud and security company SSP Europe, which is known for its secure data exchange platform, Secure Data Space. One of his customers has already been affected by this and has spent two million euros in Asia. A "chief" could convince the finance department. "It is often the case that all tricks are used, companies are often monitored for several months, the CEO's email account is hacked, and then, on a suitable day, a really big action is to be struck," says Steiner.

The highly-organized gangs know exactly, who is when and how often at a site, the callers are well-informed, well-instructed and speak the corresponding dialects, in order to gradually gain the trust. If an email is received from the right account with the urgent instruction to make a lightning transfer, in order to cut and dry the takeover and the chief financial officer signs this project, the chance is great that is passed. The chance to see the money again, is extremely low.

Education and transparency

Good IT security systems could prevent such refined attacks. There is also a lot of awareness training with the employees, clear rules, transparency, and a business climate, which allows employees to report their own mistakes and strange things immediately. Because the dark side is disposed at all times. Every day, more than 150,000 viruses are roaming the Internet, causing more than one million people in the EU to be victims of cyber attacks. According to the IT security provider Kaspersky, 58 percent of the world's computers in corporate networks were infected by a malware attack in 2015 at least.

According to security specialists, the biggest mistake is the predominant approach by most of the SMEs, that nothing has ever happened and the own company is not interesting enough for crooks. According to the "Symantec Security Report 2015" about one third of the attacks are against companies with less than 250 employees. Behind most cyber attacks, such as the currently very popular blackmailing/crypto trojans (Ransomware) are often fully automated systems, which simply look for badly secured systems. One click on a wrong email or fake website and the malicious software is enclosed in the system, to cause damage immediately or to work themselves up slowly to the decision makers with high IT security clearance.

Can hit anyone

Even the well-known US security company RSA, which also serves some customers in the defense sector like Lockheed Martin, was victimized in one of the most sensational cybercrime cases in 2011 by a perfectly targeted phishing email. What has been stolen has remained secret, but it has certainly been highly sensitive data from some 15,000 customers. With spear phishing, targeted employees are selected, in order to lure them with social engineering tricks- for example clicks on a spam mail, which is actually rated unsafe, but at times some mails are rejected by strict spam rules or interesting wording.

According to a study by Verizon, 23 percent of employees click on emails with interesting sounding attachments such as "planning2015.xls" or "payroll.xls", other eleven percent open the attachments. This makes the system prone to attacks. Combined with new vulnerabilities in software programs - here a malware in Excel - and tools from the Darknet fate takes its course. Slowly, the cyber-crooks work their way up the network, crack the IT administrators' passwords, spy privileged users with keylogger that record every keystroke, and cameras. If there is enough information, the perpetrators watch for the perfect point in time to manipulate payment transactions, or even take over cash machines, which then provides money.

Big estimated number of unreported cases

The accurate number of frequency and strength of companies harmed by cyber attacks is limited.. In the normal case, cyber burglaries and other security incidents tend to swept under the carpet in order not to damage their reputation. According to the statistics in the report on "Internet Security in Austria 2015" by CERT.at, the Austrian National Computer Emergency Response Team, 10,884 relevant reports and 10,425 reports of real security incidents like phishing occurred last year.

The server-paralyzing Distributed-Denial-of-Service attacks areas strong as the blackmail trojans. According to the security experts, never pay any bills outstanding , since the right key is only rarely delivered. Sometimes security experts can save the data here. However, some companies have already been deprived of their foundation of a contract by an encryption attack. In this case, there are already very cost-effective backup solutions from IT security companies, which, if not previously detected by the Trojan, still save the data from encryption.

Counterfeit bills

The domestic industry in particular has recently been hit by the "Spoofed Invoice Fraud", where invoices from long-standing international business partners are sent again with a new account connection shortly after the charge. According to CERT, around half a dozen such attacks occurred in 2015 on companies that were financially damaged around a six- to seven- digit Euro- Amount.

It is therefore important to know where the original emails come from, because for such actions often badly secured internet servers are captured. A Domain Monitoring of the own company names is an effective defense, products & websites as well as a clear security management, precisely defined security processes (e.g., in the case of extraordinary payments, dual control principle, direct telephone contacts to the superiors to inquire) and the definition of an incident response & communication strategy. In addition to modern virus scanners and firewalls, the latest security architecture also focus on proactive security systems (such as Advanced Persistent Threat Tools and Security Information & Event Management) that monitor and analyze data flows using big-data tools, keep up-to-date on the latest Internet threats and alert in the case of threat immediately. This System is offered by numerous security specialists and large IT corporations such as SAP and Co .

Simple and effective measures

Large, comprehensive security systems are, of course, also a question of cost. Often, the measures to increase security significantly are very simple. For example, encrypting emails or digital signatures, keep a lot of damage away and is also cheap.,

1. More secure in the Cloud?: Particularly small and medium-sized enterprises can hardly afford or manage highly secure data centers and IT systems. Certified cloud vendors have long been more secure, and security experts are constantly working to paralyze the latest methods of hacking. "Our cloud also shields companies from encryption trojans and prevents data loss through backups," says Andreas Dangl, Managing Director of Fabasoft Cloud GmbH, which recently became the first cloud provider to receive the highest certification from the European Cloud organization EuroCloud. But there is already Security as a Service-IT security for companies fit as a cloud solution.
2. Who am I?: The most important thing in digital business is to really know who to communicate with. For this the it must a safe bet that own e-mails are of oneself. Thereby most Internet attacks are already in vain. "A two-factor identification should already be standard in companies in critical business areas," emphasizes Edgar Weippl, Research Director of SBA Research, the largest IT security research institute in Austria. In addition to the password, an confirm SMS on the mobile phone or an identity card should be

mandatory. "Even with conferences organized by us, some speakers are called to make credit cards for hotel bookings," says Weippl. In turn helps only elucidation. In any case, a consistent identity and access management is the core element of any IT security architecture and let many security problems underdone arise. Procedures that are simple and inexpensive, such as digital signature, multi-level authentication, etc., help.

3. Employees: The majority of security incidents are triggered by employees - usually unintentionally or through negligence, but sometimes through targeted industrial espionage. Here, training, clear guidelines as well as a company culture help, which appreciates if one's own mistakes, which can happen once, are passed on quickly.

4. Smartphones and Co.: A big danger are all mobile devices, especially own, unsecured mobile phones, notebooks and co. On the one hand the data and the data transmission (for example via public WLANs) are badly protected, on the other hand, spies may be look over the shoulder and rustle passwords.

5. Holistic concept for security: Cyber-crooks always aim at the weakest link in a system. " A comprehensive security concept as part of an IT strategy - not Insolutions-helps", says Franz Grohs, CEO of T-Systems Austria. IT security and the IT transformation should always be top priority.

The original article can be found at http://www.report.at/home/aufmacher/item/89343-top-prioritaet-sicherheit-schnell-mal-eine-million-ueberweisen.