What the Hack!

Burning dough ...

The worst-case scenario following a cyber attack according to engineers at a Canadian biscuit factory? “Salty biscuits, but no worse than the loss of a day’s production”, was their answer. Unfortunately, they were completely wrong.

In 2015, production at a Canadian biscuit factory ground to a halt after hackers infiltrated its network. The cyber criminals used software to analyze the factory’s network and take control of its sensitive PLC (programmable logic controller) systems. Production stopped, and the biscuit mixture that had already been produced dried up in the transport tubes. The blockages caused by the mixture were so bad that the pipes had to be disassembled and replaced, leading to severe business interruption for the manufacturer.

Although malfunctions are part of everyday life for a production technician, malicious manipulations are not. Protection of industrial control systems has to be improved urgently, otherwise worse can be expected than dried-up biscuit mixture. Just imagine if the target had been a medicine factory, or if a city's drinking water supply were manipulated.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

I could have cried ...

In 2017, a ransomware attack known as “WannaCry” affected more than 200,000 computers globally. Individuals, businesses and organizations in over 150 countries were reported to have been affected. The WannaCry attack exploited a known vulnerability in older versions of Microsoft Windows. Although Microsoft had released a fix for this in March after the vulnerability had been identified, not all systems had been updated. The malicious software may have been downloaded onto computers via links in emails. WannaCry also appears to have the capability to spread between computers that have the same vulnerability. Affected businesses and computer users were faced with a ransom request of US$ 300–600 in bitcoin to restore their systems. The greatest impact appears to have been on healthcare services.

The biggest issue facing businesses and users is the inability to access their systems and data, causing disruption in productivity whilst systems are restored to working order. Ransomware attacks are not new and have been identified as one of the fastest-growing trends in cyber crime. Incidents are multiplying at an alarming rate.

This time, greater damage was prevented only by the courageous intervention of a young British citizen. The 22-year-old discovered a vulnerability in the malicious software: by registering a website, he was able to leverage the Trojans and stop the ransomware spreading further.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

Dangerous wildlife

In 2007, the hacker group APT28 (Advanced Persistent Threat 28), also known as “Fancy Bear”, made its first public appearance. They specialize in targeting prominent institutions and appear mostly in political contexts. In the beginning, experts encountered several malicious programs – some of which developed by the group itself. During the Caucasus conflict, several Georgian ministries were hacked by the group. But that was just the start: in 2014/15, Fancy Bear systematically infiltrated the defense ministries of several European States: Bulgaria, Poland, Hungary, Albania and Denmark.

In 2015, Fancy Bear infiltrated the IT systems of the German Bundestag. The offices of at least 16 parliamentarians were combed through, mail boxes copied, hard drives scrutinized and internal data – some of it likely classified – misappropriated.

›

Just a year later, the infiltration and data breach of the US Democratic Party during Hillary Clinton's election campaign were attributed to APT28 by the FBI. Their latest appearance was in 2017, when the campaign headquarters of French presidential candidate Emmanuel Macron were hacked. Finding proof on the internet is difficult, but US intelligence services and others say that many clues point to Russia.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

Target: Vital functions

In the past few years, healthcare data has become the most valuable asset for hackers. And healthcare institutions have thus far been insufficiently protected against cyber attacks. Medical practice and hospital servers host sensitive patient data and disease documentation and are permanently connected to the internet. According to a study by the Ponemon Institute (2015), each medical record is worth about €320.

In August 2014, the systems of the US "Community Health Systems", an association of 206 hospitals, were infiltrated and 4.5m medical records were stolen, including names, social IDs, addresses and telephone numbers.

Around the turn of the year 2015/2016, 28 German hospitals were victims of cyber attacks. Two of the attacks were critical: hackers managed to infiltrate computer systems with a malicious software that encrypted all data. In Neuss, the attack was accompanied by a blackmail attempt. Both hospitals had to completely shut down their IT networks in order to eradicate the viruses.

In this era of digitalization and digital healthcare, cyber attacks can literally threaten the lives of patients all over the world.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

Pickpocketing 2.0

Following a spectacular cyber attack on the central bank of Bangladesh in February 2016, further attacks on financial institutions have taken place, with the international payment service provider SWIFT also being hacked. It is not known how much money was lost during the latest attacks.

In February 2016, hackers had tried to steal a billion dollars from Bangladesh's central bank by manipulating SWIFT transactions. It appears that the perpetrators hacked into computers with which SWIFT messages are sent and requested transfers of large sums from Bangladesh Bank's account at the New York Federal Reserve. Although most transfers were blocked, the hackers captured US$ 81 million – transferred to casinos and casino agents in the Philippines.

At least US$ 15 million of the stolen funds were recovered with the help of the Philippine Anti-Money Laundering Council.

According to investigators, the Bangladesh central bank had not protected its computers with a firewall and had used unsafe hardware systems. Requests by Bangladesh Bank officials for SWIFT and the New York Fed to take some responsibility for the cyber heist were rejected. SWIFT had initially insisted that the security of the global payment system was not compromised. But there have recently been reports of further attacks. SWIFT is used by around 11,000 financial institutions worldwide.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

Locked in vacation

Hackers had been trying for months to infiltrate the IT systems of an Austrian luxury hotel. Finally, in December 2016, they gained access to the hotel's computers and encrypted all data, including backups. It appears that – months before – an email had contained malicious software. Since then, hackers have targeted the hotel's IT infrastructure on four occasions.

Two attacks were thwarted, according to local newspapers. In December, however, the hackers managed to bring the key card system under their control, locking all doors in the hotel. The hackers demanded a ransom of €1500 in bitcoin and, in the end, the hotel administration decided to pay. The company suffered losses of around €10,000 and the hotel management immediately implemented security measures.

›

All computers that do not necessarily need an internet connection were disconnected, and data backups are now saved offline to prevent remote access.

Another attack took place at the end of January 2017. But this time the hotel's security defenses successfully blocked the attack. The hotel's management is currently considering replacing the chip cards with regular keys.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

Unbreakable steel

In 2014, a German steel mill was the target of a cyber attack. Hackers took control of the production software, causing significant material damage to the site.

The attackers first hacked into the site's office software network by sending so-called phishing mails and infiltrating the system with malicious software. They proceeded to penetrate the steel mill's production management software, taking over most of the plant's control systems and methodically destroying its components. They succeeded in preventing a blast furnace from initiating its security measures on time, causing serious damage to the infrastructure.

›

The hackers' motivation is still unclear. Nonetheless, this attack was classified as an advanced persistent threat. Most APTs are linked to groups backed by sovereign states. One can thus wonder what the aim of such an attack really was. If cyber attacks are able to cause damage to infrastructure, then populations can also be impacted. An attack on an electricity production facility, for example, could cause power outages for hundreds of thousands of people. Digital infrastructure is already the battleground of some present-day conflicts, and most certainly will be a major one in the future.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

Dangerous liaisons

In 2015, a major online dating website for married people was hacked by a group that identified itself as “The Impact Team”. The hackers threatened to release users’ personal information if the site was not taken offline. The operators – a Toronto-based company – announced that they had removed information from their site that could be used to identify users but, soon after, exactly that sensitive information was leaked online.

The names, postal and email addresses, phone numbers, genders, dates of birth, profile captions, weight, relationship statuses, sexual preferences, credit card information and transaction history of 30–40 million users of the dating service were published. As a result, the company lost about a quarter of its annual revenue, there were reports of suicides, resignations and marriage break-ups, and official

investigations. The results of those investigations were released in a report, which noted that the company's security measures were lacking; its use of a fake security verification was deceptive; personal information was illicitly retained after profiles had been deactivated or deleted; and that the company did not adequately ensure the accuracy of customer email addresses.

Shortly after, a national class action was launched against the owners and operators. This lawsuit was filed on behalf of all Canadian residents subscribed to the website. The plaintiff claimed US$ 760 million in damages.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

The same old trick

In 2017, hackers were able to break into the electronic patient files at an old-age home in Switzerland. Once they gained access to the computer system, the hackers proceeded to encrypt the patient files and block staff from accessing the data. Luckily, management had kept hard copies of the files as a backup, so that the health of the elderly patients, who are of course particularly dependent on planned and regular care, did not suffer as a result. According to the facility's director, he nevertheless ended up paying the ransom demanded by the hackers in order to regain access to the data.

The case demonstrates that the age-old hacking trick of encrypting data still works. And health data are a particularly lucrative target, since there are good chances that the victims will pay the ransom, and multiple systems are often linked in the health-care system's cyber infrastructure. Security gaps therefore often open up at the interfaces between the various systems. Selling hacked data has become so lucrative for criminals that "cyber crime-as-a-service" offers have even begun to appear, with the purpose of cracking the security architecture at companies in the health and pharmaceutical industries. The risk affecting that industry is thus particularly serious – and is growing steadily.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

No such thing as a free lunch

A woman from Germany suspected nothing when she recently transferred €2,200 to what she thought was the revenue office.

Little did she know that her online bank account had been hacked beforehand by a trojan horse, to make it look as if she had just received a deposit from the revenue office in that amount. Not only that, but the hackers also froze her online account altogether. They then sent her a fake e-mail stating that she had received the money by mistake, and asking her to "transfer it back" to the tax office. Local media have reported numerous similar cases.

Hackers are getting cleverer all the time. Where they used to steal data mainly through spyware or phishing, cyber criminals are now turning to increasingly complex fraud scenarios such as the one just described. And the victims usually end up empty-handed. It is not difficult to imagine how losses might skyrocket if such professional scams start becoming widespread.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

Closed due to hacking

A workplace that has to remain shut, dozens of PCs blocked and unusable – every manager's nightmare recently became a reality for famous research institute in Bayreuth. Why? The "Locky" trojan horse had infected one single computer inside the institute's network, blocked access to the data, and then proceeded to attack other workstations over the network.

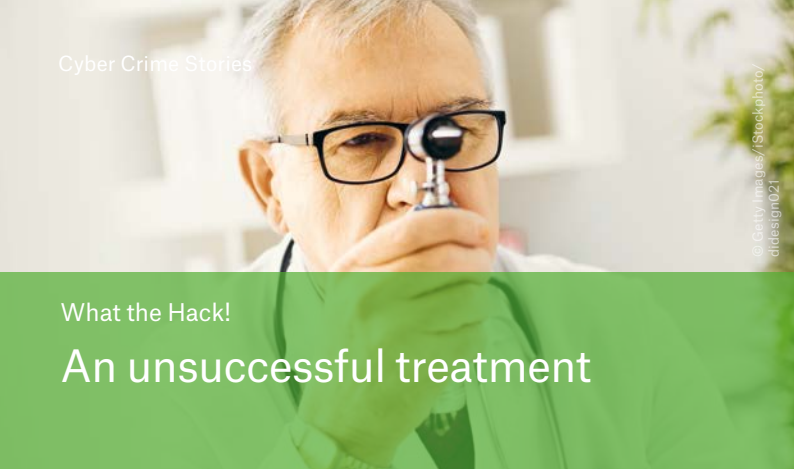
The hackers then demanded a ransom in bitcoins to release the computers, which was to be transferred via specially created pages on the victim's network. Locky had gone viral in the truest sense of the phrase: experts estimate that it initially affected over 5,000 systems per hour in Germany alone.

›

Its main carriers were infected text or spreadsheet file attachments. The malware also used manipulated websites to infiltrate victims' computers.

Locky caused tremendous damage worldwide, presumably because the hackers had painstakingly planned their attack: they had prepared versions that clearly explained, in the victims' own languages, how they could regain access to their data – another example of how cyber criminals are becoming increasingly sophisticated. And the unfortunate moral of the story is that such hacks remain a significant and increasing risk, especially for companies with large in-house networks and multiple clients.

Why chance it?
Get in touch with your Client Manager at Munich Re.



What the Hack!

An unsuccessful treatment

A doctor near Munich was on the lookout for new staff recently, when he received a personalised e-mail from the employment office with a list of suggested candidates. Unfortunately for the doctor, the e-mail turned out to be neither from the real employment office, nor was the attachment what it seemed to be. Instead, with one double-click on the attachment, hidden malware seized control of his entire IT system, including 73,000 patient files and access to his storage backups, external data servers and health insurance accounting system.

Upon paying the ransom, the dentist then got an unwanted introduction into the world of bitcoins from the hacker himself.

Instead of releasing the data upon payment of the initial €4,000 ransom, however, the hacker proceeded to demand another €6,000.

To add insult to injury, the malware not only blocked access to the doctor's servers, but also destroyed their structure so that the entire operating system had to be rebuilt – adding another five figures to the total damage. It took almost a month and a half before the office was able to use its IT again.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

911, What's your emergency ...

In 2018, a hack forced Baltimore's 911 dispatch system to be temporarily shut down. The incident was classified as a ransomware attack during which hackers take over parts of private or municipal computer networks and then demand payment, or ransom, for their release.

The attack was made possible after an IT team troubleshooting a communications issue with a server unintentionally changed a firewall, leaving a port open. Hackers likely were running automated scans of networks looking for such vulnerabilities, found it and got in. "I don't know what else to call it but a self-inflicted wound," said Frank Johnson, chief information officer in the Mayor's Office of Information Technology. "The bad guys did not get in on their own without the help of someone inadvertently leaving the door open."

The breach shut down the city's computer-aided dispatch (CAD) system, forcing the city to revert to manual dispatching during the breach. And 911 calls were not recorded in the dispatch log for almost 24 hours.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

It wasn't me ...

A person's identity is their most valuable possession, especially in the age of online shopping and banking. Consumers use their address, phone number and other personal details to keep transactions secure. That's why identity theft – when this information gets stolen – can have an enormous impact.

In the US, the largest ever case of identity theft occurred when an employee at a software company sold consumer data to a network of criminals. The passwords and codes enabled the gang to download thousands of credit reports – and to cause losses of between US$ 50 to 100 million by using the information to perform financial transactions. But identity theft isn't always an inside job: In 2009, hackers took advantage of security weak spots to steal 45.5 million debit card numbers from a payment processing company. Within just twelve hours, they

had withdrawn more than US$9.4 million from around 2,100 cash machines in 280 countries worldwide.

It is vital that security systems are strengthened to protect private information, because identity theft has the potential to cause a massive amount of financial damage very quickly – and victims also suffer emotionally because the data is personal.

Why chance it?
Get in touch with your Client Manager at Munich Re.

What the Hack!

Automobiles at a standstill

A major car manufacturer and their partner company found computer screens in multiple smart factories displaying the dreaded Bitcoin image and ransom demand. The damage began when the “WannaCry” worm encrypted files and froze PC access at a facility which stopped all activity and halted the production work of 3,500 employees. Since the virus can reach across interconnected networks, two factories along the value chain as well as an interconnected partner company were forced to cease production.

The companies’ losses for remaining offline, paying idle workers over a number of days and IT restorations far exceeded the initial ransom demand of US$300. With a shutdown costing each factory millions of dollars per day, security risk prevention for probable IT interruptions would have been invaluable. And at hand, too: The security patch that could

have prevented the standoff had been available for months.

As machines-as-a-service and IoT devices become the norm for Industry 4.0 manufacturers, IT-centred strategies to risk are becoming the frontline defence against attacks.

Why chance it?
Get in touch with your Client Manager at Munich Re.