The Cyber-Pandemic

IT Attacks in the Healthcare Sector

pandasecurity.com

panda

The Cyber-Pandemic

There is no industry that can be considered more noble or selfless than healthcare. Its character is so humanitarian that, even in situations of conflict, they will respect and protect you in any way they can. It is very difficult to think that someone would want to disrupt the public value of the healthcare industry, let alone deliberately target them with very serious cyber-attacks.

Money is the engine that moves the world, but unfortunately, it overlooks classes, conditions or sectors. Money is the main motivation for many cyber-criminals who have discovered in healthcare the mother-lode of vulnerable industries.

The healthcare sector is focused on other concerns which is probably why they have may have neglected their IT security for so many years. We find ourselves with a technologically advanced industry with neglected IT security, and that is extremely disturbing.

A Compromised Background

Ransomware has become one of the most prevalent threats today. This is one more example that shows us that money is a major driver for cyber-criminals. An attack that targets victims with valuable information, and who are willing to pay ransoms for the retrieval of that information, makes ransomware the perfect weapon.

We have seen attacks designed against a specific industry. In fact, in certain industries such as the financial sector, a hacker's interest is more than obvious, to empty bank accounts of money. Even when the victim is the actual bank, the objective is the same, as we saw recently in the case of the Central Bank of Bangladesh.

Other sectors may not suffer from the direct theft of money, but the goal is still very clear. As documented in the recent "The Hotel Hijackers" whitepaper, the cyber-attacks on stores, services and hotels went after customer credit card data by infecting the Point of Sale terminals.

However, in the health sector the motive is not so obvious. In many countries, it is not common for the patient to use credit cards to pay for services, either because the services are funded by the government or through private health insurance. In spite of this, hospitals, clinics or labs are increasingly often victims of cyber-attacks.

Why healthcare networks became targets of cyber-criminals?

In accordance with the Office of Civil Rights of the United States, **during 2015 there were some 253 security holes in the healthcare sector which affected more than 500 people with more than 112 million records stolen**. This industry suffered more attacks in 2015 than any other sector, according to IBM.

They are the heart of a technological revolution. The healthcare industry is moving to store all information electronically which is, without a doubt, beneficial for the patient and caregivers alike.

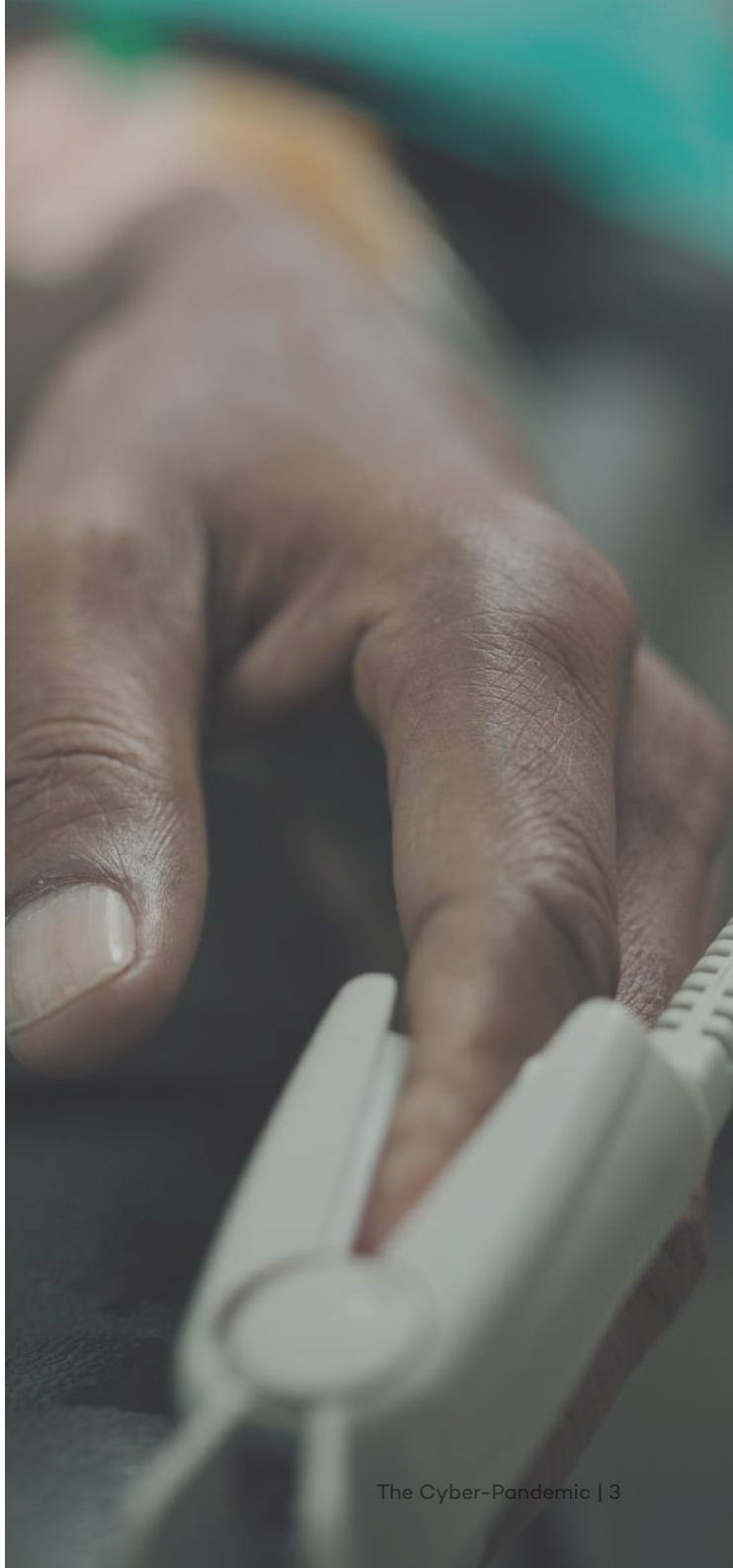
This information is available on a network to be used in the event of changes, like a change of doctor, and it can be easily accessed by looking at the patient history. This convenience is the same thing that has generated a serious security problem for the healthcare industry. Medical information is very valuable and highly-sensitive, so whoever controls this data can strike it rich.

In some countries you can trade this stolen information, and there are even companies that are interested in buying this type of data, from research centers to insurance companies. Then of course, there is the black market, where a clinical history can be much more valuable than credit card data.

Medical records contain a large amount of personal information, which might be used as the master key to carry out future targeted attacks. Think of the main people in positions of power, who are especially cautious with their privacy, and refrain from disclosing personal information online on social networks, etc. Even those who are very careful cannot prevent medical centers from keeping their records on file. If this confidential information falls into the wrong hands, like those of a cyber-criminal, their personal data will no longer be so private.

Another example could be gaining access to confidential information from pharmaceutical studies, where the competition would pay large sums for the opportunity to take away a patent from their competitors. Or another less exaggerated example, could be to obtain the private information belonging to any doctor which could be used to illicitly prescribe medicine.

Medical histories, test results, email addresses, passwords, social security numbers, confidential employee information, patients and company data: all of them are incredibly valuable and are surrounded by the latest technology. The problem is, **they are protected with a security system that is now obsolete**.



A History of Lucrative Attacks

American Red Cross

In 2006, an employee at the American Red Cross in St. Louis stole the identities and information belonging to three blood donors. The consequences could have been far graver because this employee had access to data from more than 1 million donors.

Accessed more than 1 million donors' data

Temple Street Children's University Hospital

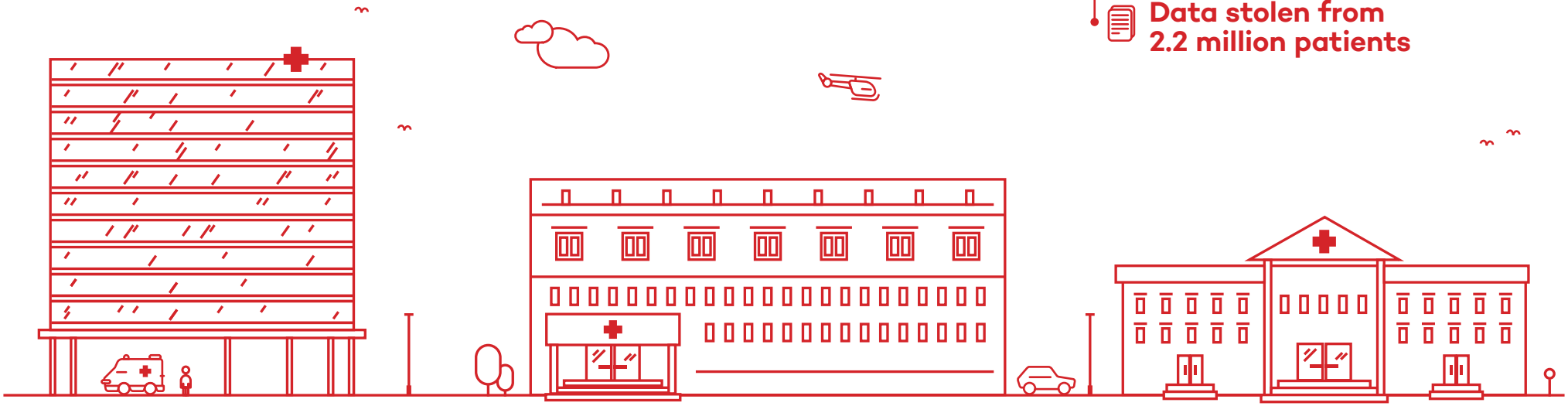
A year later, two servers containing data from almost one million patients were stolen from Temple Street Children's University Hospital in Ireland. The servers contained patient data, including names, date of birth and reason for admission.

Data stolen from 1 million patients

The University of Utah Hospitals & Clinics

In 2008, the University of Utah Hospitals & Clinics announced that data belonging to 2.2 million patients was stolen. The data was stored on backup tapes that were left inside an employee's car, who worked for an external storage company which the hospital had contracted. In this case, the employee failed to comply with the established protocols for the transport of the information and millions of people's private data was compromised.

Data stolen from 2.2 million patients



Until now we have only discussed specific cases, not large-scale attacks. However, with the passing of the years, the landscape has changed dramatically. **According to a study published by the Ponemon Institute, in the last five years, attacks in the healthcare sector have increased 125%. Cyber-attacks have become the main cause of information loss.**

This situation is worrying, especially since 91% of organizations reviewed in this study have suffered at least one attack that has resulted in data loss over the past two years. 40% have acknowledged five or more data loss events over that same period.

Anthem Insurance Company

One of the most infamous attacks in this sector took place in February 2015. The second largest Insurance company in the United States, Anthem, suffered an attack that led to the theft of 80 million customer records, where extremely sensitive data such as Social Security numbers was lost.

Apart from information theft, and the possibly of it being sold, we should also take into account the ransomware attacks which have direct economic impact on victims. Establishments like hospitals, pharmaceutical and insurance companies have such a large quantity of highly valuable information that ransomware attacks have affected this sector with special virulence. Cyber-criminals are focused disproportionately on them. They are constantly looking for more opportunities to hijack this information so they may later reap the rewards.

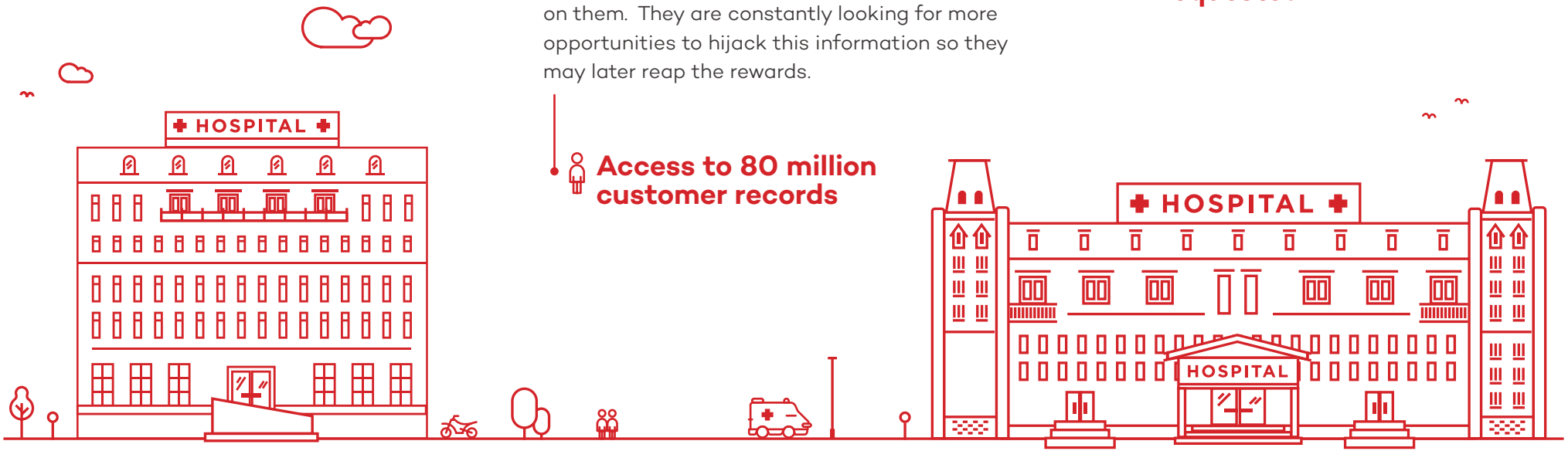
Hollywood Presbyterian Medical Center

In February 2016, the Hollywood Presbyterian Medical Center in Los Angeles declared an "internal emergency" as their employees were left without access to patient medical records, email and other systems.

As a result, some patients could not receive treatment and had to be transferred to other hospitals. The ransom payment requested by cyber-criminals was $3.7 million. Eventually the hospital's CEO came to an agreement and paid approximately $17,000 to be able to retrieve the abducted files.

$3.7 million was requested

Access to 80 million customer records



Baltimore MedStar Health

The following month Baltimore based MedStar Health also admitted that they had to disconnect some of their hospital's systems due to a similar attack.

They have to disconnect their hospital's systems

Henderson Methodist Hospital

The Methodist Hospital in Henderson, Kentucky was another victim.

In this case, an unconfirmed ransom of $17,000 was paid, although it was speculated that the payment could have been considerably higher than this figure.

$17,000 was paid

Prime Healthcare Management

Major US provider Prime Healthcare Management, Inc. was also a victim to cyber-attacks. Two of their hospitals were attacked by cyber-criminals (Chinese Valley Medical Center and Desert Valley Hospital), forcing network shutdowns, and many other facilities were affected by this very same attack. In this instance the company did not pay the ransom.

Two of their hospitals were attacked

Lukas Hospital and Klinikum Arnsberg

American hospitals are not the only target. German hospitals have also been victims of similar attacks.

According to the international broadcaster, Deutsche Welle, several hospitals suffered ransomware attacks, like the Lukas Hospital in Neuss and the Klinikum Arnsberg in North Rhine-Westphalia. Neither hospital paid the ransom.

Several German hospitals have been attacked

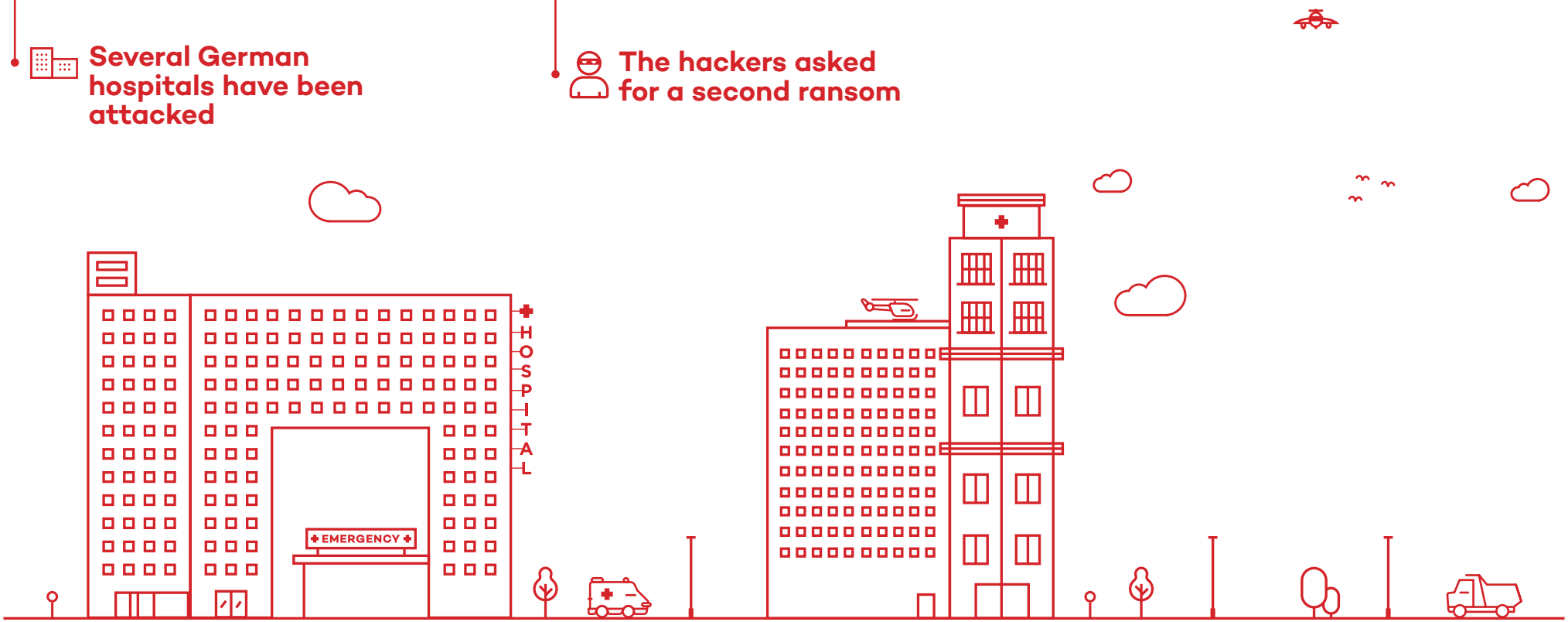
Kansas Heart Hospital

It should be noted that paying a ransom in any of these examples does not ensure that your information will be returned. A clear example of this is the ransomware attack on Kansas Heart Hospital in May 2016. The head of the hospital decided to pay the ransom but the attackers, having realized the value of the data, demanded a second payment to recover the rest of the information. The hospital decided not to make the second payment.

The hackers asked for a second ransom

"Prevention is better than cure"

With all these cases in the healthcare sector they should listen to their own advice.



A Science Fiction Reality

As shown in the above examples, these types of attacks are fully capable of shutting down a hospital by denying access to these files, robbing thousands of logs and holding the sensitive information hostage.

Underneath all of this, there is something much closer that affects all of us. Practically all medical equipment (pacemakers, scanners, X-ray, infusion pumps, respirators, etc.) are connected to a network. It is very real that these medical devices could in some way be hacked.

In 2013, former U.S. Vice President Dick Cheney revealed that his doctors disabled wireless communication on his pacemaker because they saw that it was highly possible for someone to remotely attack his device if they wanted to.

A year before, Barnaby Jack, a New Zealand hacker, demonstrated to security conference attendees how **a pacemaker could be hacked remotely, producing a life-threatening electric shock**. Barnaby designed an attack that could affect all pacemakers within 15 meters.

He had also demonstrated how a portable insulin pump, used for diabetes patients, could be altered remotely, making it possible to inject a lethal dose of insulin to all appliances in a 90 meters radius.

Jack died a week before being able to demonstrate how to hack artificial hearts. In The Black Hat Conference 2013, he would have revealed how to alter the pace of these implants.

X-ray, Scanners, Respirators,...

Medical devices that are unprotected right now.

A pacemaker was hacked

by an attack that could send a mortal shock.

Insulin pumps were altered

to inject a lethal dose of insulin.

Richard Rios also took into his own hands to reveal the vulnerabilities in medical devices. A polyp in his respiratory tract left this investigator at the Stanford Hospital for two weeks. During this time, Rios realized that his bed was connected to a computer. There were also belts which raised his feet and an infusion pump that injected his medication on a daily basis. He investigated and found up to 16 networks and eight Wi-Fi hotspots without leaving his room.

After lying in bed for a few days, he got up and moved to the aisle to stretch his legs. On this short walk, he discovered a computerized drug dispenser. The responsible for all medicine distribution was actually a computer, which doctors and nurses controlled using a coded identification card. Before noticing the appliance, Richard had already figured out that this system had a vulnerability: a password embedded in the source code of the program (hard-coded password) allowed others to "play" with the drug dispenser.

Along with his partner Terry McCorkle, Richard has identified more than 300 vulnerable devices in some 40 different companies in the social-healthcare environment. The names of these companies were never made public but Rios is sure that these vulnerabilities still exist today.

In his eagerness to demonstrate the danger posed by these security holes, **Richard Rios was able to demonstrate how it is possible to remotely manipulate the medication pumps** used in hospitals throughout the world. He hacked several of these devices to alter the medication dose to a lethal level. Rios warned that this could be done on more than 400,000 of these pumps throughout the world that remain vulnerable.

Almost at the same time, several analysts at TrapX Security in San Mateo, California, began to track vulnerable devices across more than 60 hospitals. **They infected hundreds of devices with a program that replaced part of the original operating system of the device in question**. The infected machines remained fully operational, so nobody realized there was a problem, but those six months allowed TrapX to monitor all hospital activities on the network.

Among the devices that they had access to were x-ray machines, blood and gas testing machines, pumps and, of course, computers used by the medical team. Many of these computers had unsupported operating systems and as such were more vulnerable, like Windows XP or Windows 2000.

The fact that the anti-virus protection of the majority of these hospitals did not detect the TrapX infection, suggests that their devices were not protected very well. They remained infected until TrapX Security sounded the alarm.

Uncontrolled drug dispensers
that allow to play with the distribution of the medicines.

400,000 Medication pumps can be altered
to modify the infusion flow of its medicines.

Hundreds of infected devices
that remained infected for months.

How could have these attacks been avoided?

We have seen how criminals carry-out attacks to steal sensitive information, medical histories, pharmaceutical studies or data belonging to insured persons. We've seen how they access e-mail addresses, passwords and social security numbers without problem. Or how ransomware kidnaps vital information that can cripple the activity of an entire hospital, to make money.

Avoiding these far-fetched attacks is not a simple task. What we are implying is that a set of actions are put into action: resources and policies designed specifically to safeguard the security of devices, data and people.

The first recommendation is basic and crucial: **depend on a cyber-security solution with advanced protection capabilities and the ability to detect and remedy possible threats**.

Something shared by the majority of these attacks is something simple to explain yet complicated to obtain: the lack of control over what happens in computer systems. We recommend that you **depend on a model that is capable of controlling all of the active processes on the devices that are connected to the corporate network**.

Having total visibility of what happens will allow you to control any anomalous behaviour in your systems and to act before the damage occurs.

Additionally, companies that handle sensitive information should **review their personnel policies and control systems to adjust the privacy requirements and adapt them to the available technology**.

Our last piece of advice is something we always reiterate and that is far simpler than it seems, and is rarely taken: **we must always keep all of our business operating systems and programs updated**. This way, the doors will be closed to all known vulnerabilities, thanks to the correction patches that are released by the manufacturers.

It is good to have an updated policy and control of the available devices. This type of management system has monitoring and inventory tools that can help us make equipment and system maintenance more effective, uniform, centralized, and secure.

The solution

To protect against advanced threats and targeted attacks we need to have a system that guarantees Data Confidentiality, Privacy of Information and Business Reputation, and Legacy.

Adaptive Defense 360 **is the first and only cyber security service that combines the most effective traditional antivirus and the latest advanced protection with the capability of classifying all executed processes**.

Adaptive Defensive 360 can detect malware and strange behaviors that other protection services cannot because it classifies all running and executed processes.

Thanks to that, it can ensure protection against known malware and advanced Zero-Day Threats, Advanced Persistent Threats and Direct Attacks.

With Adaptive Defense 360, you will always know what happens to each of your files and processes.

Detailed graphs show everything that takes place on the network: timeline of threats, flow of information, how the active processes behave, how the malware entered the system, where it is going, who intended to do what and how they got that information, etc.

Adaptive Defense 360 makes it easy to discover and fix those vulnerabilities while also preventing the unwanted (like navigation bars, adware, add-ons...).

Adaptive Defense 360: limitless visibility, absolute control.

More info at:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

More information at:

BENELUX
+32 15 45 12 80
belgium@pandasecurity.com

BRAZIL
+55 11 3054-1722
brazil@pandasecurity.com

FRANCE
+33 (0) 1 46842 000
commercial@fr.pandasecurity.com

GERMANY (& AUSTRIA)
+49 (0) 2065 961-0
sales@de.pandasecurity.com

GREECE
+30 211 18 09 000
greece@pandasecurity.com

HUNGARY
+36 1 224 03 16
hungary@pandasecurity.com

ITALY
+39 02 24 20 22 08
italy@pandasecurity.com

MEXICO
+52 55 8000 2381
mexico@pandasecurity.com

NORWAY
+47 93 409 300
norway@pandasecurity.com

PORTUGAL
+351 210 414 400
geral@pt.pandasecurity.com

SPAIN
+34 900 90 70 80
comercialpanda@pandasecurity.com

SWEDEN (FINLAND & DENMARK)
+46 0850 553 200
sweden@pandasecurity.com

SWITZERLAND
+41 22 994 89 40
info@ch.pandasecurity.com

UNITED KINGDOM
+44 (0) 844 335 3791
sales@uk.pandasecurity.com

USA (& CANADA)
+1 877 263 3881
sales@us.pandasecurity.com

Adaptive Defense 360

Limitless Visibility, Absolute Control

pandasecurity.com

panda