Why healthcare IT security is so hard

By Leif Nixon,
Security Expert at Sectra Communications

The problems surrounding IT security in the healthcare sector are causing increasing levels of concern, both among healthcare professionals and in regulatory bodies. Over the past six months, there has been a steady stream of flash messages from the FBI, the Department of Homeland Security and other security organizations about increased threat levels against healthcare systems. We have seen a multitude of healthcare provider organizations falling prey to ransomware attacks, putting patient safety at risk and causing enormous financial damage. But why is this sector experiencing an increase in attacks? Is there something specific about healthcare that makes IT security particularly hard? Yes. Yes, there is.

Safety versus security

The concepts of safety and security are closely related, yet distinct. While safety is about protecting against random failures and mistakes, security is about protecting against malicious attacks. There are few areas where these two concepts are as intricately interconnected as in healthcare. Add to this the fact that the data handled in healthcare systems often has very serious privacy implications and you get a swamp of problems to which there are seldom any perfect solutions—only imperfect compromises.

A concrete example: Privacy regulations like HIPAA and GDPR declare that medical records are highly sensitive information and must be carefully protected. This has given rise to security requirements stipulating that only authorized individuals who have been securely authenticated may access the record databases. However, from a safety perspective, having prompt access to medical records can literally be a matter of life or death. In a medical emergency, there is no time for screen locks or forgotten passwords.

In practice, the compromises employed to solve this conflict between security and safety tend to range from elaborate “break glass” systems, where the normal access control can be bypassed in an emergency, to the more directly pragmatic solution of placing the computer mouse in a blood bag rocker that flips it back and forth, so that the screen lock never activates.

A trefoil of systems

There are also aggravating circumstances in the form of the uniquely tripartite structure of healthcare IT systems. Of course, all healthcare providers have everyday administrative office systems for tasks such as email and spreadsheets. This aspect of healthcare IT is shared by all large organizations. While the problem of protecting these kinds of systems might not exactly be solved, there is at least a sizeable, shared body of knowledge and best practices for how to deal with them.

Bigger healthcare providers also have large numbers of networked medical devices. These range from infusion pumps and insulin monitors to high-end MRI scanners, all hooked up to a computer network for the purposes of monitoring, data sharing, and remote access. These devices are subject to strict safety requirements that are often incompatible with basic IT security practices, such as frequent software updates. Indeed, many medical devices contain embedded computers that run operating systems that are no longer supported by the manufacturer. An IT security engineer might demand that such insecure systems be placed on a fully isolated network, only to quickly discover that this is not possible since the staff requires access to medical data from their office workstations. In addition, many hospitals and clinics have established contracts with specialist providers, such as teleradiology companies, that operate in different time zones to simplify coverage during off-hour shifts. Thus, there is a need to transfer MRI scan results to specialists on the other side of the world.

Beneath a healthcare provider's administrative systems and medical devices lies a third, often forgotten, system: the supervisory control and data acquisition (SCADA) system that controls the infrastructure of the hospital or clinic. All the facilities that we take for granted, such as heating, ventilation, electrical power, lighting, and water supply, are all controlled by specialized computer systems. These are critical for the hospital or clinic to function, but seldom draw much attention from an IT security perspective. Yet there are plenty of realistic and frankly frightening scenarios to consider.

For example, if a ransomware attacker figures out how to target the engineering workstations for the heating and ventilation systems, they could easily stop all major surgery at a hospital by shutting down ventilation to the operating theaters and then disabling the workstations. An attacker that gains access to the power control systems may well be able to take out both primary and reserve power, likely leading to life-threatening situations within minutes. And the list of nightmare situations goes on.

An abundance of regulations

While the technical reality of healthcare IT systems is complex, the regulatory environment in which they exist is a veritable labyrinth. Take, for example, a typical system for the distribution of medical oxygen, in which the gas is led in pressurized pipes throughout a hospital. In a normal setting, the physical pipework will be the responsibility of the facilities staff, while the gas itself is a medical product that is the responsibility of an appointed nurse or physician. In addition, there are industry safety codes for any handling of pressurized gases, which require that an internal gas safety organization be established. It is extremely unclear which of the multiple stakeholders involved has the ultimate responsibility for the IT security of the gas distribution control system.

With unclear chains of responsibility, there is an increased risk that issues will fall between the cracks, and it becomes harder to enforce a uniform IT security policy.

Ransomware, the nemesis

Given all of the above, it should not come as a surprise that many healthcare organizations turn out to be fairly porous targets for a determined attacker. However, most attackers expect some form of monetary gain from their attacks. While stolen medical records have always had a certain value in the marketplace, it was not until the advent of large-scale ransomware operations in recent years that the IT security threat to healthcare organizations really began to rise.

An ordinary business organization that is hit by a ransomware attack may—out of a certain sense of civic-mindedness or out of pure spite—simply refuse to pay the ransom, which means that all the time and effort the attacker has put into the attack is lost. A healthcare organization, however, will normally be under enormous pressure to restore its systems since patient safety is at risk. For a sufficiently brutal attacker, targeting healthcare organizations simply makes good business sense since they are more likely to pay up.

> If a ransomware attacker figures out how to target the engineering workstations for the heating and ventilation systems, they could easily stop all major surgery at a hospital by shutting down ventilation to the operating theaters and then disabling the workstations.

Indeed, while a large portion of ransomware attackers have publicly stated that they will refrain from attacking healthcare organizations during the COVID-19 pandemic, other groups have intensified their attacks, since a victim that is already under pressure from the pandemic will be even more likely to pay the ransom. Of these latter groups, the Russia-based Ryuk gang may be the most notorious, and has figured prominently in warning bulletins issued by government authorities.

A solution, my kingdom for a solution

Unfortunately, there are no easy solutions to the healthcare IT security crisis, no magic black box you can simply hook up to the network, no five-step checklist to solve all your problems. One would wish that IT criminals could simply be put behind bars, but many—or most—operate from rogue jurisdictions such as Iran or Russia, where they are untouchable.

This will be a long journey and all stakeholders need to pull together. Not only must device manufacturers learn how to improve device security and law enforcement agencies how to collaborate internationally in an efficient manner—healthcare organizations must also learn how to continuously improve their security in an incremental fashion.

However, while there are no easy solutions, there are at least some basic guidelines for improving your security.

Chief of these is the realization that you are never done. You are up against motivated and intelligent adversaries who will come up with a steady stream of new ways to attack you. The saying “security is a process, not a product” is not just a cliché. It is also true.

Also remember that security needs to be improved in a balanced manner. If you spend all your budget on improving medical device security, you are not really much better off because the bad guys will simply attack your office network instead. You can safely assume that the attackers will always go for your weakest point.

And, finally, don’t forget those SCADA systems!

Sectra AB • communications@sectra.com • communications.sectra.com

This is a marketing material and may be changed at any time without prior notice.
Sectra will not be held liable for any errors or misconceptions herein.

SECTRA
Knowledge and passion