stars insights: 21 June 2019

Missing Cyberhygiene: Ransomware – Curse and Cure

*Earlier this week, **Martin BOSSHARDT**, CEO of Open Systems, a globally leading provider of software-defined networking in a wide area network (SD-WANs), received a group of Friends of stars at their headquarters. Bosshardt explained how Open Systems combines network and security with threat intelligence and incident response to secure business-critical applications for global businesses. One dominating topic is ransomware. Media-savvy campaigns like WannaCry have reminded network administrators and board members alike that IT infrastructure is, in fact, critical. Yet ransomware is only the visible and painful symptom of an underlying problem: missing cyberhygiene, writes Dr. Serge DROZ, VP and Chief Scientist of Open Systems Computer Emergency Response Team.*

The curse
In 1854 the London neighbourhood of Soho was struck by a cholera epidemic. Within only one week more than 500 people died. At the time, the "miasma theory" explained that the spread of the deadly disease was due to bad air. Foul smells were supposedly responsible for infecting the people, and recommendation for a cure included enough red wine.

At the time, the physician John Snow wanted to know better and went to people asking them about the disease. He carefully plotted his findings on a map of Soho and could trace the origin to the Broad Street pump station. He concluded from his data that this was indeed the water pump, and not something else, because he noticed that the workers from the nearby brewery did not get sick as they did not drink the water from the pump. Snow's findings eventually convinced the city council to remove the pump handle, thus ending the epidemic. It still took another generation for Robert Koch to identify the germ responsible for cholera. Today, no one doubts that proper hygiene, i.e. water purification and proper wastewater management are the only effective measures against waterborne diseases.

What is obvious in the physical world still seems to be completely ignored in the virtual space. Almost all security experts today would agree that proper internet hygiene is a key

element in protecting our ICT infrastructure. Yet, malware seems to have been infecting our computers at epic rates for many years. Only recently, boards have become alarmed, because a few years ago a new underground business model was rediscovered by cybercriminals: extortion! Ransomware sends our infrastructures to a grinding halt, and most often it seems that the only available option is to pay the ransom, fuelling cybercrime even more. While traditional malware is hard to spot, and the damage it causes is often not very visible (some data lost here, some money stolen there), ransomware cries out loud. Boards, suddenly faced with very concrete facts, are calling for a quick cure and many cybersecurity outfits are quick to answer with the electronic equivalent of snake oil.

But this will not work, it will give you a break until the next wave, and possibly a statistical fluctuation will give the impression that the remedy actually worked.

The cure

State-of-the-art managed security services can protect more than a million endpoints and greatly reduce the chances of infection. The reason for this is neither a magic bullet nor secret technology – it's a proper security setup operated by professionals. Network access is protected by firewalls. Traffic that is allowed into the networks is scanned by web proxies and mail filters and monitored by an Intrusion Detection System (IDS). Different network segments of an organization are separated and connected through secure SD-WAN technology.

But there is bad news: attackers have begun to realize that data which is well protected is probably valuable. Today, there are underground services available that camouflage malware, so it is not detected even by up-to-date signatures of the antivirus engines. Attackers manipulate the end users, exploring humans' tendency to help and tricking them into installing malware. Or they attack a supplier with lower security standards to trick their way in. This is what happened in the Petya case, where an update server of a third-party provider was compromised.

Keeping an eye on and having the entire, continuously expanding network under control requires special solutions, such as the use of SD-WAN and the support of reliable service providers with a high level of know-how in IT security for enterprises.

Thus, protecting the perimeter is no longer enough. It is still necessary – the bad guys banging at the front door don't just go away. But to defend against current threats, the endpoints need to be part of the plan. This implies that organizations should know their endpoints, which surprisingly is often not the case. Analysing your network logs should tell you what is around though. Furthermore, endpoints need to be secure and up to date. Vulnerability management today is a must. It may well be that a patch cannot be applied to a certain server for whatever reason. So other measures can be taken. But not knowing the patch levels of your infrastructure is what made WannaCry so successful – missing or misconfigured firewalls allowed it to reach systems and exploit a security hole that could have been closed two months previously. Updated systems, correct segmentation would have stopped the spread of the malware, and a functioning backup process would have aided the quick recovery.

Bypassing network defenses is feasible, as we have seen. So, the only option is to catch attackers on the scene of the crime, the endpoint, preferably before they get to your crown jewels. This is where a properly managed endpoint detection and response system comes into play. The tool allows you to detect suspicious activities and stop attackers before they

create damage. In the case of ransomware, this means detection and isolation of an infected system before it encrypts all your network shares. This implies around-the-clock monitoring, as unfortunately, miscreants do not stick to office hours. The infected system is probably lost, but most of your data should be safe. And restoring a system and few megabytes of data is not quite the same as restoring your entire data centre. Think about a cholera-infected person returning from a bad holiday trip versus an entire infected neighbourhood.

And should an incident occur in spite of everything, professional incident handling is necessary to minimize damages and get operations back up quickly.

So, more technology? Yes and no. As attackers become more efficient, more tools and infrastructure are necessary to keep them in check. Yet what is needed even more are people with enough insight and know-how to make good use of these tools. Managing detection rules of an Event Data Recorder (EDR) system, or processing thousands of indicators per day is no easy feat. Most organizations are not willing or capable of operating an effective security team. They are best advised to leave the job to professionals.

Talking of professionals: John Snow was able to pinpoint the source of the epidemic using statistical methods, a century before this became standard in the medical sciences. In security, using data science methods is considered as a magic bullet. However, data science is what the name suggests: a science. Understanding your data, i.e. your logs, allows you to discover shadow IT, anomalous behaviour and much more. But you need to understand the data in context, just as Snow did nearly 200 years ago.

As the eradication of cholera implied building infrastructure and changing habits, so does defending against cyberattacks. In the ICT realm, this means a thorough security infrastructure from perimeter to endpoint operated professionally, together with an emergency plan to handle incidents effectively. Only proper network hygiene and a working detection and response will keep you and your data safe.

Open Systems is a leading global provider of a secure SD-WAN that enables enterprises to grow without compromise. With assured security, AI-assisted automation and expert management that free valuable IT resources, Open Systems delivers the visibility, flexibility and control together with the performance, simplicity and security that businesses need in their networks.

The views expressed here are solely those of the author and they do not necessarily represent or reflect the views of the stars Foundation.

stars insights are exclusive contributions by business leaders and experts who scan the horizon to discuss geopolitical, economic, technological and further trends and developments which will impact society and business in the next few years.

STARS – FOR LEADERS OF THE NEXT GENERATION
Rathausstrasse 33, 8570 Weinfelden, Switzerland Phone +41 52 540 00 20 info@the-stars.ch www.the-stars.ch