The security perimeter is gone, phishing is triumphing and ransomware is rampant - A realistic perspective on cybersecurity

Users do stupid things, IT managers do stupid things, and criminals are getting smarter. The answers are limited to the elementary and the adoption of new technologies such as artificial intelligence and isolation.

Diario IT 19/04/17 7:06:57 Something is totally wrong with cybersecurity. There have been two decades of investment in hardware, software and security services, and what do companies and governments have to show? Which we have seen to be a continuous succession of security breaches. Successful ransomware attacks range from hospital records to police investigation data. Personal information from school teachers has been stolen in order to use it for identity theft. They light up the accusations of cybernetic actions sponsored by governments.

Everything from social networks to mobile phones to cloud-based services are vulnerable to cyber crime. Fortunately there are new areas of innovation that could reverse the situation, offering the potential to give victims (or potential victims) the ability to defend themselves. Or, if you prefer, not to defend yourself but to have as much efficacy as possible to prevent cyber attacks.

The fundamentals of security matter

Why is cybersecurity still such a formidable problem? Is it because the "good" do not have the right tools, or have not bought the right technology? "On the contrary," said Dave Lewis, a security consultant, whose view the real reason is that companies are not maintaining good practices, such as keeping up with software patches and security alerts. "The only thing that I think is a fundamental problem is our inability as defenders to do a good job making sure we have all the patches up to date, that we are monitoring the connections, and we know that it is circulating through our networks."

Lewis continued: "Consider the breach that affected Target. They had all the tools. They had everything they needed. Unfortunately, no one was paying attention to the tools; That is to say, the main task of the defenders was not being fulfilled. We can buy all the boxes with multicolored lights, subscribe to all imaginable services, but nothing changes the fundamental problem of attitude towards computer security. "

"The challenge of having a secure foundation is that, well, security is a complex problem that can not be simplified," said Lloyd Webb, Sales Engineering Director at Cylance . "Complexity is a natural consequence of what we are doing. It is our scope of action. We are dealing with complexity. It's almost like complaining that the sea is wet. Because in our organizations we do more things, whose diversity is increasing, we also increase the surface of attack. Now this can be seen as a mathematical version in the layers of software development, in terms of how many ports are actually open, and that can be attacked. "

One of the main reasons for this complexity lies in the interfaces between different parts of systems, which Webb calls edges. "These are the edges between the chip and the operating system, between the operating system and the applications, between the applications and the users. We have more and more edges to be present in our task; Therefore, this is an opportunity for some intruder to enter a digital wedge that allows him to enter his organization. "

Webb added that "Meanwhile, the old threats continue to appear as well. We are not solving all the problems as we go along. We solve some, but not always. Take, for example, the SQL injections. Although we know perfectly well how SQL injections work, they are still used as a form of attack. "

"We definitely have a problem if we stay in the basics," said Anton Grashion, Senior Director of Product Marketing at Cylance. "However, we are spurring a dead horse if we believe our users are going to do the right thing. They are constantly doing the wrong thing. We need to empower them with technology to help prevent some of these things from happening. Although user education and awareness are important, we should never expect them to do the right thing. They always do the wrong thing and I do not think we should blame them for that. "

There is no perfect solution, no magic products

Jason Steer, architect of solutions for Menlo Security , referred to a common belief: "That if we only find the right product, the ultimate solution, your company will be safe. Something I've seen as a vendor of security technology, is that many customers think they can plug the fundamental security cracks with paper. You can not expect a product that solves a piece of the puzzle to solve the whole puzzle and therefore, if I buy this product now I will be sure. "

The same point was echoed by Carl Gottlieb, CTO & Founder of Cognition. "Every customer who has ever bought something like antivirus has said to himself: 'this is good' - but then if they suffer a gap they realize that they do not like it and future will look for a different product." Why? "People are buying poorly sold technology because no vendor will admit where their defects are."

The result, Gottlieb insists, is the lack of credibility in the industry, which is a problem because customers are just as interested in honesty as in the specificities of the particular technology product. "Therefore, something I constantly see is customers asking who are the most honest sellers? Who are the ones who are really showing credibility in either the channel or the market in general? Customers are truly connecting with those who demonstrate credibility. "

Track - and automate - definable and repeatable processes

Picking on the subject of wrongdoers: "We've been talking about automation as the cure for human error for the past 30 years," said Steve Broadhead, founder and director of Broadband-Testing. "Several levels of automation have been achieved, but there is still nothing, in general, to prevent people from deliberately or accidentally causing a problem. So how can the industry prevent people from doing something stupid when their intent is not to cause harm? "

"Define repeatable processes," said computer security consultant Lewis. "This is an old concept that constantly goes unnoticed in IT environments. If we have identified the defined and repeatable processes, we can lower the incidence rates. That allows us to spend more time working on projects that are relevant to the organization. "

It's potentially potentially affecting the entire industry, Lewis said. "It's not a stupid user case. Because they are not. They know what they need to do. The problem is rather that they sometimes need help in defining their needs and requirements. If you sell them a product that does not help them, they will get angry, bother, cancel the order, comment the situation to their friends, and these to theirs; In conclusion, a setback for the seller. "

Webb, of Cylance agreed, referring to the incessant false positives that flood many security equipment. "If you've had an attack and you're being inundated by all these alerts, it's really a matter of volume. How can you, in such a situation, really identify the truly relevant everyday elements? So if we can help reduce some of that noise and really identify for them the most important things, maybe with some automation, that's where we need to go as an industry. "

Who makes decisions about processes, procedures and protocols? "That can be problematic," said Jason Steer of Menlo Security. "We often ask users - and I'm not talking about security professionals - to make decisions about incidents against which they have no capacity to make decisions. In my own case, many years ago, when I first installed a personal firewall on my PC, I constantly received messages that this or that IP address wants to connect to this or that other port using this or that service, allow yes or no? Sure why not? Yes, let yourself go. "

Phishing often works, unfortunately

"In the business environment, employees at all levels are under pressure of time to do their job, including processing large volumes of e-mail," added Steer. "That's why a lot of phishing attacks work, it's because people need to do their job. It is human nature. If you allow people to make mistakes, then they will. We need well-defined processes. But you also have to automate some of those processes, because if you have a policy impossible to meet, then you have a problem, because people under pressure will do strange things. "

"While phishing is a huge problem, we should not only worry about email," said Dennis David, founder, CEO and president of Agenda LLC. "They make a phone call and apply social engineering: 'Hey, I'm Dennis from your IT department. I saw that you had problems with your email. What is your password?' You would not believe how many people tell you your password without any problem. "

Incidents of this type can be very costly. "In 2015, a company called Ubiquity in Silicon Valley suffered $ 40 million in losses from that type of fraud," Cilling's Grilling said. "The CFO received an email from the CEO asking him to transfer money to an account in China. The fraud was successful because it was late on Friday and the CFO wanted to leave the office. The fundamental gap was that no one made a single check. The CFO did not call the CEO to ask you, did you actually send me this email? A simple phone call would have revealed the breach. Time and again we find that if there is something that the attackers do very well it is to find the gaps in the process to detect where the weakest link is. "

Another example was provided by Gottlieb of Cognition, who raised the case of a human resources employee trying to fill a job as a matter of urgency. "Their job is to consider new candidates for the organization, and that means studying CVs and referrals. Meanwhile, the security manager tells you that you should never open documents in PDF or others from people you do not know. So, what is valid? You have two policies that are in conflict. "

The answer, according to Gottlieb and others, lies in technology. "Malware is a technological problem that we can solve to allow people to do their jobs, to enable them to help the business," he insisted. "It's a technological solution. We can train people as much as we want, but everyone will click on an email on their phones, without examining it thoroughly, because that is the reality. We have to admit that training is irrelevant. Technology is the first line of defense and that's where we have to focus. "

Ransomware: Effective but buggy

"Ransomware is another new name for an old problem," said David of Agenda. "Ransomware is equivalent to malware that is usually entered via email, usually a phishing campaign, and when the user clicks on the wrong item, ransomware is installed."

What happens then? Operating in the background, ransomware will silently encrypt everything it can see and then try to send that information to the control unit. The ransomware controller then tries to extort the user and after the victim pays criminals will decrypt the data - in theory. "Not always," David said. "The problem is that a lot of the malware is not written very well, so it can not be taken for granted that it will work. Half the time, they will not be able to find your encryption key. They can encrypt your data and send the key to the control center, but it simply does not receive it, so they can not provide the decryption key to the organization being extorted. Therefore, even if the victim pays, nine out of ten times will not recover their data. In that case,

And the odds are that if the lost or stolen data involved financial or customer information, the security breach means that the affected organization has incurred a breach of laws.

Compliance with laws is not the same as observance of security

Many large organizations focus on compliance with current regulations, demonstrating that their procedures, policies, and technologies conform to government regulations, privacy standards, or industry standards. Simply because an organization can demonstrate that it is complying with applicable regulations does not mean that the organization is safe, but it is a start.

"Do not look at compliance with the mentality of marking the appropriate boxes, to make sure it will not be sued," advises consultant Lewis. "Look at it rather as a vehicle to drive security within your organization. You can use compliance to get a budget and then push projects for security. " Lewis noted that such observance is simply a reference to external norms: "It is only the minimum. Use compliance as an element that helps to better secure the organization. "

Mener Security's Steer said, "Companies today want a closed, one-word answer to a problem that is much more complex than legal enforcement. It will take years of lessons learned from noncompliance. These are the right processes, these are the right controls, these are the right measurements, these are the right outputs to measure something that most companies do not have now. CIOs and CISOs should be able to say, 'No, we're not sure. We will never be safe, 'without fear of losing his job. "

"From the point of view of cybersecurity, people and companies need to understand that cybersecurity and legal enforcement are two different elements," said David de Agenda. "They are related, but they are not the same thing. There are situations of data protection, which is something totally different from the protection of security. "

David continued: "Cybersecurity ensures that your network is secure, that your users can safely use the services and tools you provide, while not losing their data."

Perimeter? What perimeter?

Broadhead of Broadband-Testing pointed to emerging solutions to urgent security issues, and while none of them are in the miracle formula category that can solve the security problems of an entire organization, they can provide valuable protection in a way Which ancient technology could not achieve. As an example he cited the revolution in perimeter protection.

"You have guys who have been investing in firewalls and related technology, filtering over the past 15, 20 years," Broadhead said. "And now they come across a company that says, 'No, that's not the way to do it, that does not work anymore, you need to use this.' How do you explain that to a CISO? "

Cylance's Webb said, "The hard perimeter you could fortify has disappeared. There is no perimeter anymore. These are multiple layers of protection and do the right thing for the user. One of the most important things in the industry right now is back to prevention. What can we do to prevent further attacks so we can have the people, the time, and the resources to focus on the things that really matter to an organization? "

David, from Agenda, agreed. "Vodafone lost the phone numbers and banking details of millions of people. Most errors like these, if not all of them, were committed because someone within your network, some of your users did something they probably should not have done, either accidentally or deliberately, and also because the old has disappeared Adagio of just having a solid perimeter and a great firewall is left out to all bad guys. Things do not work that way anymore. "

Artificial Intelligence and Isolation

Artificial intelligence is a tool used by Cylance and others to focus on prevention, said Grashion of Cylance. "AI is a tool that is at an evolutionary stage, and there are some things that really fits well and some things where it is probably less suitable. It evolves with automatic learning, neural networks and new advances. "

"I always use the analogy of a nail gun," continued Grashion. "You can use a nail gun to place nails quickly, or you can use the nail gun's end as a hammer. You can use the tools appropriately and inappropriately. At the moment I can not even see an application where AI would be inappropriate. But if we do not innovate, if we do not keep the innovation curve to the rhythm of the malicious actors, then we are really in a game that we will lose because we are going to lag behind more and more. "

Menlo Security uses a new approach called isolation, which assumes that all files and websites are malicious and opens all sites and documents in a secure, isolated cloud environment that protects endpoints and enterprise networks from malware. "Isolation focuses on prevention, without trying to determine good or bad behavior. After all, we have 20 years of firewalls, antivirus, sandboxes, trying to determine good and bad behavior, and have failed. Taking a step back and not having to rely on those data to decide whether something is good or bad is refreshing because we give up the idea of having to discern. We turned something that was malicious into something safe. "

Just because you build a better mousetrap does not mean people are going to buy it, said Gottlieb of Cognition, who set the example of distributed denial of service (DDoS) attacks, stressing that although technology is available to stop them, it is not being widely available Adopted. "What can we do with DDoS? A lot. You can protect yourself against DDoS very, very easily if you pay for the service. The challenge is that no one is paying because they do not value it enough. "

Keep your head up to avoid problems and find solutions

It is easy to feel overwhelmed. There are so many attacks, so many malicious agents, and so many solutions on the market - and tons of claims about miracle solutions that will solve all your problems, regardless of your needs. What should you do? Solve the requirements, then talk to the sellers ... even if that means many, many sellers.

Cylance's Webb said, "Many customers are overwhelmed by vendors who call them and tell them they can solve their problems. There are newer security startups than at any other time in the history of Silicon Valley. From the east coast and the west coast of the United States to Israel, there is an incredible level of innovation. "

Maybe too much? Webb said, "I met a CIO last week who said 'I have 50 salespeople telling me they can solve my problem.' He does not even have time to talk to two of them, but he has 50 chasing after him to offer his help. My reaction would be to close the blinds and say, wait until next year and see what happens then. "

One place to look for answers is the cloud, said Steer of Menlo Security. "There are numerous benefits to migrating to the cloud. However, from a customer perspective, they are not too sure of being ready for the cloud yet. Companies assume that they can only replicate what they have done at their own facilities for 20 years and assume that they will be able to do the same in the cloud, when they do not. But companies apply a 20-year model of legal compliance, risk, and security - and they think that's still making sense in the cloud. It is not like this".

A final tip from David, from Agenda: "People need to be aware of what is going on around them, that is, look up and see what is happening, rather than looking down like the sheep they normally are . In fact, they are heads looking at the screens of cell phones. But if you look up and see what is happening around you, then you can really identify the problems. They could bypass that security hole and avoid falling if they really look up and see what's going on. "

By Alan Zeichick

Spanish version, exclusive for TI

About the Author

Alan Zeichick is a software engineer and systems analyst. He has worked as a writer, editor, and technology analyst since 1980. He was founder of SD Times and co-founder of Network Magazine, along with serving as chief editor of LAN Magazine and editor of Computer Security Journal. His work has also been published by the Computer Security Institute.

Although we know perfectly well how SQL injections work, they are still used as a form of attack.

Lloyd Webb
*Sales Engineering Director, **Cylance***

We often ask users to make decisions about incidents against which they are unable to make decisions.

Jason Steer
*Solutions Architect, **Menlo Security***

LAST NEWS

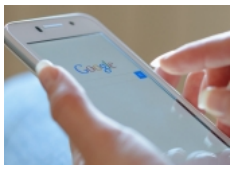
Are they listening? The dangers of voice assistants

Making the leap: the first applications of SDN and NFV demonstrate the need for integral and practical alliances

Red Hat launches Red Hat OpenShift Container Platform 3.5

Microsoft will slow apps on Windows 10 to improve battery performance

Huawei seeks to grow in the cloud despite intense competition



Google loses control of Android in Russia

Gartner: "PC sector contracts"; IDC: "the sector grows"

Cybersecurity is not only technology but also laws

Mobile devices to lead digital shopping

Categories

Big Data | Contact Us | English | Government | Hardware | IoT | Mobility | Network | Cloud / Cloud | View Ti | SDN / NFV | Privacy Policy | Software |

Contact