UBM

E-PAPER

FEBRUARY 2015

Cybersecurity – You're Already Compromised

Threat Intelligence Would Have Told You Sooner

Level(3)® COMMUNICATIONS

IN COLLABORATION WITH

Alcatel·Lucent

Corporate spending on IT security reached a record $71 billion in 2014. This represents an 8% increase over 2013, and it's predicted to increase another 8% in 2015. With an accelerated increase in spending on cybersecurity, year over year, you would think companies are winning the battle against cybercriminals – but they're not. Virus infections, network penetrations, and data breaches continue at alarming rates, and with greater consequence.

It's becoming clear that throwing hardware and software – and ultimately more money – at the problem doesn't work. Given the potentially high rewards, cybercriminals are motivated to work together and learn from past successes to stay ahead of traditional IT defenses. That's why you need to explore less conventional methods of security that combine threat detection, prediction, and containment. Threat intelligence is a vital strategy that will help you achieve this.

The Sad State of Cybersecurity

Each year, IT faces an increase in targeted cyberattacks, more sophisticated and prepared attackers, a significant increase in DDoS attacks, and a growing number of hacker toolkits and black market trading sites for stolen data. Add to this the growing use of cyberattacks for use in espionage and geopolitical statements, and the future of cybersecurity looks even grimmer.

In addition to the increasing number of incidents of data breaches – where critical data is stolen – the average time a hacker goes undetected inside a system is on the rise as well. Research by Verizon shows that 66% of all breaches remained undiscovered for months or longer. Additionally, according to George Kurtz of CrowdStrike, the average malware infection lives more than 200 days before detection. With more than 2.47 million new mobile malware samples collected in 2013, up 197% from 2012, this problem will get worse.

In fact, James Comey, Director of the FBI, has pointed out that there are two types of companies: those who've been hacked, and those who don't know they've been hacked.

When implementing an effective security strategy, understand that your data is a valuable asset. Know its value, location, and movement at all times.

Next, know your adversary. For example, attackers can be hacktivists working to make a political statement or protesting a cause your company may be associated with, or they may be thieves attempting to sell your data or hold it for ransom. The cybercriminal might even be a nation-state looking for trade secrets, or an insider looking to exact revenge.

Next, know why they're hacking you. You need to know the hackers' motivation, what they're looking for, and how they might get it, which goes back to understanding the value of your data. Make no mistake about it: Your business is neither too small nor too large. You are actively being targeted. Once you know where you stand, deploy a strategy using common security practices and implementations. It's important to perform regular security evaluations and risk assessments, and to provide awareness training for your employees.

Companies must perform regular security evaluations and risk assessments and provide training.

Here's the dilemma: According to Level 3, the cost to implement a traditional cybersecurity defense will continue to rise, and it's still not enough to stop the bad guys. In a way, this endless increase in spending is also a waste of money, time, and resources. Consider that a majority of all breaches are discovered by nontechnical efforts, with 88% discovered by external parties (outside your company and your security systems), according to Verizon's 2014 Data Breach Report.

In terms of cybersecurity, instead of spending more, you need to spend smarter.

Spend Smarter: Implement Threat Intelligence

No doubt, you still need proper perimeter security, with appliances, applications, and processes in place. But what do you do when the problem continues to get worse, even as your budget increases? What if budget or economic constraints require you to spend less on security? With the current trends, most companies are digging themselves into a deeper hole.

As you increase your security buildout, you also have more infrastructure to manage and update. Ironically, over time, maintaining your security implementation can actually become a distraction from protecting your organization from cybercriminals.

Surprisingly, you can actually spend less and improve your security if you spend it in the right places. Begin by developing a risk-based approach to manage threats and vulnerabilities. Next, establish and adhere to a governance, risk, and compliance (GRC) discipline and framework. Most of all, you need to implement threat analytics.

Leveraging data gathered from network traffic, application, and user behavior, coupled with predicative analytics, threat intelligence helps you identify threats and breaches shortly after they occur, or just as they begin. To implement it, you need the right governance and organizational structures in place, brand new security strategies, collaboration, and the right algorithms and analytics. Above all, you need the right partner.

Just as the human body uses a multisystem approach to intruder detection and response – i.e., hygiene, outer skin, white blood cells, antibodies, and so on – data hygiene takes the same approach. The

HISTORIC HACK: SONY 2014

Regarding the hack on Sony in late 2014, where terabytes of data were stolen and then systematically leaked, ex-Anonymous hacker Hector Monsegur's analysis leads him to believe it had been years in the making: "For something like this to happen, it had to happen over a long period of time. You cannot just exfiltrate 1 terabyte or 100 terabytes of data in a matter of weeks," Monsegur said. "It's not possible. It would have taken months, maybe even years, to exfiltrate something like 100 terabytes of data without anyone noticing."

Monsegur also believes it may have been an inside job. An employee or contractor with access to internal servers or databases of information could have downloaded and sold the data to someone on the outside.

human body has multiple reactions and defenses against intruders, and we can learn from this model. This includes building a layered defense against penetration, detecting infection in a timely manner, and using a step-up defense once infected.

To do so, you need to go beyond perimeter security and implement an advanced protection process that includes:

- Advanced detection: Analyze traffic and usage patterns to know when an attack is forming.
- Total containment: When an attack is detected, ensure that it doesn't go further.
- Threat identification: Use as a key learning tool to improve defenses over time.
- Advanced threat mitigation: This should include the removal of malware, remediation of compromised systems, and all recovery efforts thereafter.

Implementing threat analytics means becoming proactive instead of simply being reactive. With it, you can detect attacks in formation-based on patterns and past learning and, most importantly, you will be able to predict future attacks.

SECURITY BREACHES AFFECT OUR PRIVACY IN HEALTHCARE

About 43% of all data breaches in 2014 involved healthcare data, costing the healthcare industry $5.6 billion, not to mention violating the privacy of the victims involved. In 2014 alone, foreign cybercriminals stole 4.5 million patient records, proving just how valuable health records are. As a result, the U.S. government is enacting stricter requirements to report healthcare-related breaches, with greater penalties for downplaying them or not reporting them at all.

With the rising costs related to the theft of patient records, and the growing risks associated with not reporting them, it's more important than ever to stay as many steps ahead of the cybercriminals as you can. This includes the government itself, which experienced a hack attempt on some test servers related to the HealthCare.gov website infrastructure, proving security is only as strong as your weakest link.

Call to Action: Find the Right Threat Intelligence Partner

Not everyone can provide you with an effective threat intelligence implementation. Signature-based systems alone can't find these threats, especially when most are zero-day attacks. However, Level 3 Communications can be a partner in threat intelligence, given its threat intelligence strategy and global reach.

Overall, there are more than 100,000 new strains of malware distributed by over 10,000 malicious new domains each day, half of which are designed to compromise user credentials. Level 3 is in a unique position to detect and stop malware before it infects your servers. The results you get with Level 3: smarter threat detection, prediction, and more effective mitigation.

The bad guys are working together to discover, refine, and share the most effective methods and strategies to attack you. You need to do the same to fight back. Level 3 is investigating threat trends analysis, prediction, and intelligence, and it's ready to put this information to work for your organization today.

Level 3 Communications is a global communications provider headquartered in Broomfield, Colo. The company builds, operates, and maintains a global network to deliver managed solutions for enterprises, carriers, and governments, including fiber-based infrastructure and data center solutions, IP-based voice and data communications, video and content distribution, security solutions, and cloud-based data center services. Level 3 services customers in more than 60 countries spanning six continents. For more information visit **www.level3.com.**