Chief Information Security Officer best practices for 2018: Proactive cyber security

Received (in revised form): 17th January, 2018

Travis Rosiek

has nearly 20 years' experience in the security industry, he is a highly accomplished cyber defence leader, having led several commercial and US Government programmes. He is known for developing and executing strategic plans to build the technical capacity across product development, quality assurance, technical marketing, professional services and sales engineering. Prior to his role at BluVector, he held several leadership roles, including CTO at Tychon and Federal CTO at FireEye, as well as senior roles at CloudHASH Security, McAfee and the Defense Information Systems Agency (DISA).

Chief Technology and Strategy Officer, BluVector, 4501 Fairfax Drive, Arlington, VA 22203, USA
E-mail: Travis.Rosiek@bluvector.io

Abstract Cyber adversaries are adapting to the enterprise rush to include new features, add cloud and cut costs faster than IT teams are able to secure them. This cyber security paradox creates an opportunity whereby cybercriminals and adversaries only need to be right or 'lucky' once in an attack, while cyber defenders must be 'right' every time. Yet, despite the high priority of security in nearly every industry, breaches continue to make headline news. Despite effective solutions to mitigate or eliminate those threats, IT and security teams are fighting a losing battle, as the need for new features is often prioritised over the requirement for security. This paper examines these cracks in the organisational struggle for security and their root causes, and offers a practical perspective on how to achieve better defence through training, balancing processes and leveraging the right technologies to decrease attack vectors and build a proactive security process that is better prepared for current and new threats.

KEYWORDS: AI, machine learning, fileless malware, ransomware, destructive malware, training, CISO, BISO, crypto-coin mining, proactive cyber security, cyber security process

INTRODUCTION

As witnessed in the past year, cyberattacks are becoming far too common and the news is rather bleak. While the Sony and Target breaches still resonate in the minds of many globally, 2017's breaches make those well-known breaches seem pedestrian in comparision. For instance, the 2013 Target breach affected a reported 41m credit card customers and the company paid over US$162m in total breach-related expenses. In 2017, the Equifax breach stole the sensitive personal data of 145m people. And Yahoo (now part of Verizon) announced that 3bn accounts were hacked in 2013.

In 2018, with the upcoming enforcement of the EU General Data Protection Regulation (GDPR), organisations are bracing not only for any breaches but also the massive fines associated with the breach of personal data for any EU resident (including a post-Brexit UK). GDPR fines start at €10 million or 2 per cent of the company's global annual profit or annual turnover of the preceding financial year, whichever is higher.

Despite all that, one major gap that the author has continued to see over a 20 year career — and sadly does not anticipate improving in 2018 — is a sense of urgency to be proactive in cyber security. In this new era of destructive attacks, we are going to be one step closer to the 'Big One or Many' that will cause catastrophic impacts and there will not be an easy way to recover.

If organisations and consumers do not create and demand a sense of urgency and become proactive in mitigating cyber risks, then it is only a matter of time before a cyber doomsday will occur and any reactionary action to fix it will be futile.

WHY CYBER SECURITY FAILED IN 2017

The author's principal observation is that cybercriminals and advanced persistent threats (APTs) continue to have the upper hand and, in many cases, are gaining ground. The reason is simple: businesses outsourcing IT, consolidating IT systems and moving to the cloud have, in some ways, made it easier for cyber adversaries by 'putting all their eggs in one basket'.

Business decisions to save money in the short term routinely have adverse effects in the long term, especially as cyber adversaries quickly adapt to these changes. Few organisations have the required operational maturity or can maintain resources long enough to gain in-depth knowledge of the organisation's business operations to effectively protect their environments. The cyber security paradox is that cybercriminals and adversaries only need to be right or 'lucky' once in an attack, while cyber defenders must be 'right' every time. Eliminating all errors or misses on the defensive side is very challenging and not realistic. So there needs to be a holistic approach to cyber security across the entire organisation.

Looking back at 2017, we witnessed ransomware (including destructive malware pretending to be ransomware), crypto-coin mining — both likely to further increase significantly next year — use of leaked exploits (including EternalBlue) and fileless malware. The fact that 'military-grade' cyber tools/weapons fell into the hands of rogue nations and extremist organisations poses a significant risk to the global society.

In 2018, organisations will continue to be highly vulnerable to cyber breaches and all signs are pointing to an increase in the prevalence of destructive malware (ransomware, wiping software pretending to be ransomware, wiping software and Industrial Control System [ICS]-focused campaigns).

FEATURES VS SECURITY

Every year, it is easy to think there is no way that things can get worse, but again and again we are proven wrong. There are several reasons for this. In our feature-first society, we are pushed to want more features faster, and companies are incentive-driven to deliver these features as they race to innovate.

However, consumers' desire for new features and their overall lack of knowledge around cyber security and cyberthreats gives companies strong demand to build cyber security so as to ensure security is built into the products they buy. Rapid adoption of technology with countless features is great for business and growth in every way — except that all these features rapidly increase the attack surface and, in many ways, offer no easy means of remediation.

Huge shortages in the cyber security workforce globally and high turnover rates complicate the task of retaining employees who know the intricacies of an organisation's business-critical systems. In the author's experience, when tightly integrated IT operations and security operations teams have a deep understanding of what is on the network, which systems are critical, what typical system behaviours look like and how to interpret events from their various IT and security products, they perform better at thwarting red teams or cyber adversaries.

Throwing a seasoned cyber security expert or a junior analyst into a new environment typically results in a lot of educated guessing for a period of time until they learn the business, the environment and the security tools being used.

REACTIVE VS PROACTIVE CYBER SECURITY

Over a 20-year career in cyber security, one common theme that the author has witnessed is that reactive cyber security is very common because it is the cheapest path in the short term, but ends up costing organisations significantly more in the end. Ten years ago, many neither believed nor considered that cyberthreats were likely or could have a major impact; thus, they were reluctant to make the necessary early investments to proactively mitigate these risks. We have seen the significant impacts of breaches and attacks over the last few years and the impacts to business operations, brand reputation, direct impact to customers, loss of equipment and loss of corporate valuations that have reached billions of dollars.

Building a proactive and robust cyber security programme takes a psychological shift in thinking, knowledge, data and money. First, IT teams should challenge the complacent 'we are secure (enough)' mindset. With that premise in mind, they need to design their networks with an assumption that an outsider could get in, so as to build security into the environment and applications. Cyber security is not an event, but a process, so teams need to choose security tools and vendors that can evolve with their future challenges. And while no network environment exists without end users, teams need to remain ever vigilant on confirmation and access management to prevent or detect cyber adversaries from accessing your environment. Finally, test your security plan. Exercise your incident response plan across your organisation and keep it current as business operations evolve.

WE ARE SECURE (RIGHT?)

In sports, having a mastery of the fundamentals is the best building block of success. In cyber security, this building block is known as good cyber hygiene. In many of the major breaches, one major takeaway is that the organisation was fairly compliant in 'blocking and tackling', also known as 'patching', and secure configuration management.

In most cases, cyberthreats target the path of least resistance in an organisation, making it difficult to determine their level of sophistication as they often do not need to leverage sophisticated tools or zero-day exploits. Why use or 'burn' these tools if modifying tools that are already widely available on the Internet or deep/dark web will allow them to achieve their goals? As previously noted, IT consolidation is like putting all your eggs in one basket — a misconfiguration or a missed patch can have catastrophic consequences and affect the entire organisation. This creates a single point of failure in most organisations today and requires new approaches to mitigate these risks.

Compliance requirements are stagnant, dramatically lag behind cyber adversaries' tactics, techniques and procedures (TTPs) (ie how they operate) and do not address single points of failure in IT systems (eg IT consolidation). To make matters worse, these requirements are well known to cyber adversaries, who have access to many commercial security products to test their attacks, have no rules to follow and have the upper hand in the cyber domain.

Accountability has also been a problem in the cyber domain. Solely focusing on compliance has created a check-box mentality, and little attention is given to going the extra mile if the box has been checked. The main focus for many organisations has typically been achieving compliance, a strategy which has been proven time and time again to be insufficient to thwart cybercriminals or sophisticated adversaries.

EVOLUTION OF THE CISO ROLE

Historically, the chief information security officer (CISO) served as a single point of decision, authority, awareness and control across the enterprise and interacted with the security operations centre (SOC), chief information officer (CIO) and chief operations officer (COO) on a regular basis. Today, they are more focused on compliance, reporting, justifying budgets and plans to the chief executive officer (CEO) and/or corporate boards and running the SOC. More of the detailed security planning and decision making is starting to be delegated to business units and a business information security officer (BISO). The BISO has become more of a technical role while the CISO has become more business and process focused and has to influence BISOs to make change. Not having a single point person and control limits the ability to have impact for strong CISOs, but also limits poor decision making by underqualified CISOs. Hopefully CISOs and BISOs are able to influence their organisations to become more proactive over the years to come.

HOW TO TURN THE TIDE

So how do we fix this problem? The headlines in 2017 have shown us that many organisations struggle with security issues and thus enable cyber adversaries to be successful. Lack of cyber security plans, an overemphasis on being merely compliant, cyber workforce challenges and a breakdown in processes are the biggest challenges organisations face. The cyber security industry has mostly focused on providing technical solutions, with disregard for the many other challenges organisations face on a daily basis. In recent years, industry has started to react and provide solutions to help address these problems.

The key will be to get corporate boards, the entire C-Level and employees to better understand their dependence on technology, accept how at risk they truly are, and admit that reactive cyber security is no longer a solution but the problem.

Technological advancements and cloud adoption do not eliminate cyber risk, they only change the roles and responsibilities for mitigating it. That change, especially in large enterprise environments, can unknowingly open an opportunity for an adversary to gain access to an organisation's assets. They also create higher stakes for potential breaches as organisations go through IT consolidation. Consolidating information and business-critical data has many advantages, including narrowing avenues of attack for adversaries, restricting access to the organisation's crown jewels and providing an opportunity to focus on and implement specialised/customised security. However, this consolidation is often driven by cost savings rather than the desire to reduce cyber risk. Thus, very few organisations include this as part of their cyber risk management strategic plans, employ experienced security staff, or are able to retain their security teams in order to maximise the benefits of this approach.

RETAINING AND ATTRACTING CYBER SECURITY PROFESSIONALS

As noted earlier, the workforce challenges and lack of processes within an organisation are key reasons why reactionary cyber and breaches have such impacts. Recruiting and retaining cyber security professionals is an increasingly hard problem to solve, especially as demand grows globally for the talent.

How bad? ISACA, a non-profit information security advocacy group, told *Forbes* in May 2017 that it predicted that there will be a 2m person global shortage of cyber security professionals by 2019.

To add to the problem, being certified does not always mean that the individual is qualified, thereby bringing more complexity to the hiring process. The author has observed over the years that cyber security professionals want to be fairly compensated, but will more quickly leave their organisation

if they do not believe in its corporate security programme, if it does not prioritise cyber within the business, or if they are provided with tools that do not work or are difficult to operate.

Deep down, many cyber professionals have a strong desire to make a positive impact and help detect and remediate threats or problems against the enterprise.

Career growth is another key factor in recruitment or retention; this commonly consists of two flavours: upward professional mobility and increased responsibility, or the ability to move to other teams and gain new skillsets and encounter new technical challenges. Some possible solutions could be for an organisation to allow flexibility to move between teams and collaborate frequently, or offer tuition reimbursement and provide specialised training for employees to expand their skillsets. Allowing the security staff to have a say in what security tools an organisation buys also has positive effects for retention.

BALANCING PEOPLE AND PROCESSES

As noted earlier, reactive cyber security has adverse effects in the long run; not having incident response processes or letting them go stagnant also has negative consequences. The time to refresh or create incident response processes is not when an organisation is breached and working to mitigate business impacts. Having a good balance of proactive and reactive cyber security capabilities and processes is critical. If your teams are responding to a breach in the reactive mode, then they can switch to the proactive mode and begin hunting for adversaries on their networks or insider threats that may otherwise have gone undetected.

This approach can help keep your teams sharp, as they learn new skills and adversarial tactics, and greatly enhances your organisation's ability to find, confirm and contain cyber adversaries (see Figure 1).

Figure 1: A good balance of reactive and proactive cyber defence

MITIGATING DESTRUCTIVE MALWARE

It is important to know where your key data reside and who has access to the data. If your organisation does not have a stellar security programme (top 5 per cent globally), then storing all your data in one location makes the cybercriminal's work much easier. Not only should your data be backed up regularly, but the backups should be tested on a regular basis to make sure they are working properly. Many times there are issues or misconfigurations that can hamper the process for bringing information from those backups. Discovering such problems when there is a need to retrieve that data is never a good excuse.

With the rapid evolution of malware, the need to ensure that backups are stored offline or with very limited access is crucial, as ransomware such as Locky and WannaCry actually look for remote shares and backup stores. As stated earlier, proper hygiene is always important (it is very difficult to achieve over 95 per cent in organisations) and staying current with patches and a security vendor's content can aid greatly in repeat attacks where files are reused by the adversary. This is where defence in depth comes into play by incorporating

other security best practices to limit the adversary's ability to manoeuvre and move laterally across your organisation; examples include implementing a 'least privilege' culture across your IT systems and limiting the avenues of attack to your key data. Segmenting this key data on the network and focusing your security operations teams to prioritise its monitoring will greatly improve your chances of thwarting a destructive malware attack. Finally, leveraging non-signature based detection technologies, eg artificial intelligence/machine learning (AI/ML), can rapidly analyse unknown content and identify threats in sufficient time to sense and respond in minutes. The key aspect in a destructive attack is to prevent via good hygiene. If the adversary leverages a zero-day exploit or finds a crack in your organisation's security armour, speed of detection and containment is crucial.

TECHNOLOGICAL ADVANCES TO DEAL WITH THIS PROBLEM

First of all, let's discuss a brief primer on the role of AI. There are many approaches to AI, and ML is one that has been gaining traction in the cyber security domain. It was a security buzzword for 2017 and is widely used by most security vendors' marketing departments, regardless of how substantive their use of AI and ML. Vendors have used machine learning techniques on their back-end analysis for some time, but it is only recently that a few vendors have pushed AI and ML to the customer premise for real-time threat detection or post-breach detection. These capabilities are complementary as proactive and reactive uses of threat detection leveraging AI and ML. Real-time threat detection using AI/ML is focused on malicious content (file-based or fileless attacks) without use of signatures or behaviour detection engines. This approach typically works out of the box and can provide detection once deployed. Post-breach detection using AI/ML typically relies on studying the internal network traffic of network assets and users and learning what is normal and abnormal. This approach requires some period of time post-install to learn the network traffic patterns and also requires oversight for tuning within the enterprise.

One other technological advancement that gained some attention in the market in 2017 is speculative code execution (SCE), which is the exploration of multiple execution paths through machine code or scripts to identify the potential for malicious behaviour. The technique does not require, but may leverage, a control flow graph to determine paths of interest. This provides a means to detect fileless threats, even at network rates.

With the rapid increase in ransomware and other destructive malware capable of affecting an organisation immediately upon payload delivery, organisations should shift their focus to leveraging artificial intelligence, machine learning and speculative execution analytics at the point of entry into their network to deliver scalable detection and analyst efficiency. As security analysts struggle to keep up with emerging threats, an avalanche of alerts, and devices which cannot be managed, let alone patched, innovations in emerging analytics technologies will provide security professionals with the automation required to stay ahead of threats.

CONCLUSION

Proactive cyber defence must be the new normal. The time to wait is over: do not expect others to solve or stop cyber security problems within your organisation. Corporate boards, C-Levels, employees and consumers must demand that security is baked into every product and IT system, and that networks are properly designed and architected to minimise impacts in the event of a breach. Organisations must streamline processes to conduct proof of values, aka

pilots of emergent technologies, to help keep pace with the rapid evolution of cyberthreat actors. Giving tools and opportunities to cyber security professionals will go a long way to help recruit and retain top talent and ultimately will have positive impacts on reducing risk in your organisation. Finally, fostering a culture of collaboration across the organisation (not always easy) and a culture of being secure will have a dramatic effect on improving your security programme and moving the needle in the right direction for your organisation in 2018. Over-reliance on reactive security and check-box compliance are proven ingredients for catastrophic and billion-dollar impacts to organisations.