The New IT Acronym: KISSME (Keep IT Security Simple, Manageable and Effective)

Computing environments have evolved to enable users to be more productive and IT to be more agile. And yet attackers have evolved their methods too, adopting polymorphic malware to evade detection by preventive controls. Meanwhile, IT organizations continue to practice a piecemeal, reactive process of plugging holes, and it's putting companies at grave risk.

Given the nature of our dynamic computing environments and the sophistication of advanced persistent threats (APTs), a security breach is inevitable. The rise in the number of breaches over the past two years is evidence that no company is immune. As with the Target and Home Depot breaches, it's possible that malware is already sitting on your corporate network, surreptitiously exfiltrating data as you read this. The question is: How soon will you catch it?

By adding point solution after point solution, IT organizations are essentially putting up a welcome sign for attackers. IT is too busy managing controls to manage risk, so APTs enter the network undetected and hide in systems into which IT has limited visibility. Unless IT organizations adopt a new approach to security, these threats will continue to steal data and move about the network undetected.

IT organizations must stop what they're currently doing and take a smarter approach to security—one that uses the best detection and prevention methods possible to avoid an attack while still minimizing—or even eliminating—security's impact on business performance.

IDG
INTERNATIONAL DATA GROUP

Bitdefender®

THIS IS YOUR WAKE-UP CALL

There's no doubt about it: IT organizations have their work cut out for them when it comes to security. In 2014 the "State of the CSO" report, an annual survey conducted by *CSO* magazine, provided some perspective on the scope of the problem. The most significant challenges CSOs face:

- Managing security of and addressing risks surrounding mobile devices and bring-your-own-device (BYOD)
- Cyberthreats from outside the organization, including APTs and distributed denial of service (DDOS)
- Security for technology as a service and cloud computing

Although there are commonalities among these three categories, there's also a lot of variation within each one. Mobile device security is rarely a matter of managing a single platform across the entire enterprise. Users want to use the device of their choice at any time, wherever they happen to be. The risk posed by cyberthreats varies from one system to another, and no two cloud-based services share the same risk profile. Risk management becomes exponentially more complex with the addition of each new technology.

Unfortunately, studies show that the security measures IT organizations are implementing do not reflect CSOs' concerns. According to the "ISACA 2014 Advanced Persistent Threat Awareness" study, 96 percent of the respondents to its survey use antivirus and antimalware and/or traditional network perimeter technologies to thwart APTs. However, far fewer organizations address security for mobile devices and remote access technologies, both of which are increasingly being used within the enterprise, thus becoming high-risk factors.

And it's clear that IT security is getting short shrift among CIOs too. The *CIO* magazine "2015 Tech Poll" indicates that tech executives are putting investments in business intelligence, mobile apps, software as a service (SaaS) and the cloud—technologies that often open doors for more APTs—at the top of their priority list, with security applications falling to No. 6.

It is clear that IT organizations need comprehensive threat protection, but security controls must not reduce end user productivity. In addition—given the scope of the risk—management of controls must not be too complex or all-consuming for the security team.

MANAGING COMPLEXITY: KEEP IT SIMPLE

The traditional approach to security involves deploying a point solution for each part of the IT environment. This worked well enough when end user computing and server environments were relatively static. Today's computing and server environments, however, are anything but static. They are dynamic, with many facets. Deploying a point solution for each type of endpoint is costly and results in multiple management consoles. It becomes extremely difficult for IT organizations to gain insight or management control across this spectrum of systems.

It is virtually impossible to protect today's highly complex IT environments with traditional point solutions. Successful security management in the 21st century requires a new approach. IT organizations need a security solution that is comprehensive in two respects. First, it must protect the entire end user computing and data center environment, enabling a horizontal approach to securing technologies rather than a vertical approach with multiple disparate point solutions. Second, a comprehensive security solution must provide thorough threat protection—without degrading user performance. Put simply: Less is more.

There are several benefits to a horizontal approach. A comprehensive security solution gives IT the visibility it needs across all environments—be they virtual, mobile, and/or in the cloud. This is particularly important, in that many organizations are not currently logging events in these environments and

network monitoring in virtual environments is not on a par with traditional physical network monitoring and intrusion detection. A comprehensive security solution can help ensure that all of the organization's environments are being monitored and protected.

A horizontal approach also simplifies management. A single management console for all of these environments centralizes the maintenance and configuration of policies. The enforcement points in a horizontal approach implement policies by leveraging integrations with infrastructure pieces such as Microsoft Active Directory and VMware vCenter. This helps ensure consistency and compliance across all environments, including those that undergo rapid change.

Finally, replacing multiple point solutions with a single solution increases the return on the security investment—an important benefit for IT organizations that don't regard security investments as a high priority! A single solution improves IT efficiencies related to the management of security controls. It also reduces the number of vendor relationships the IT organization must manage and streamlines licensing.

ADVANCED THREATS REQUIRE ADVANCED SECURITY TECHNIQUES

As previously mentioned, a comprehensive security solution requires thorough threat protection. This means going beyond signature-based antivirus or antimalware solutions. These technologies are often reactive and fail to prevent APTs, which evade detection by constantly evolving. Enterprises need a multilayered solution that has antivirus and antimalware capabilities as well as proactive controls such as heuristics, behavioral analysis, machine learning and security algorithms that are continually fed new information. This enables security detection and prevention to evolve as fast as—or faster than—the threats they seek to thwart.

The information fed to these proactive controls must come from security intelligence gathered at a global level. Only a global security cloud that handles numerous interrogations on a daily basis has access to enough intelligence to counter APTs. The cloud must also be accompanied by a prompt immune response. All customers should be informed and protected in a matter of seconds when a threat is detected. IT organizations need a technology provider that can deliver such an intelligent security cloud.

Finally, a security solution must have only a minimal performance impact on the environment it protects. It doesn't do any good to have thorough threat protection if it negates a computing environment's cost and agility benefits. OS-based security, especially antimalware tools, can consume significant amounts of resources, which can cripple a virtual environment. Whereas virtualization centralizes and deduplicates many of the resources used by virtual machines via a shared-resources model, traditional antimalware duplicates resource consumption within each virtual machine, thereby negating the benefits of virtualization.

In the cloud, overutilization and licensing mismatches can lead to major cost escalations. Enterprises need threat protection that is built from the ground up to support virtualized environments to eliminate the bottlenecks and performance degradation that come with traditional endpoint security solutions. Through consolidation ratios, such a solution can result in a 30 percent performance increase in virtual environments.

CONCLUSION

Securing modern computing environments isn't going to get any easier. Thanks to virtualization, hybrid IT and mobile computing, the IT environment will only grow more complex, and so will security if IT organizations continue to deploy point solutions in a patchwork manner.

If organizations are to properly protect the IT environment while staying competitive and viable for their own customer base, they must address security by instituting the best visibility in systems across the entire enterprise. Point solutions won't provide this. Only advanced security techniques and a horizontal approach will do the job.

ADDITIONAL READING

Cybersecurity 2014: Breaches and costs rise, confidence and budgets are low

By George V. Hulme
CSO

In 2014, it seemed that no industry went unscathed. The data breaches this year were broad and deep. Software maker Adobe was hit for 152 million records. Online marketplace eBay was drained of another 145 million; Bank and financial services firm JP Morgan Chase 76 million; retailers Target and The Home Depot for another 70 million and 56 million records, respectively. There were numerous healthcare breach disclosures as well, such as at Community Health Services, which lost records on 4.5 million patients.

The attackers are getting creative and they are costing businesses big. In its October earnings call, eBay cited its data breach as one of the primary reasons for dramatically lower third quarter revenue growth. Earlier in October, security vendor Invincea released information on how attackers are targeting organizations in the defense and aerospace industry through highly targeted malicious advertising.

Despite it being yet another year of staggering data breaches, and as you'll see later from the 12th annual Global State of Information Security Survey 2015 conducted by PricewaterhouseCoopers and CSO, these breaches are costing enterprises more – and information security budgets aren't keeping up with the threat. In some cases, they even have fallen slightly. It's as if security teams manage to make a small foothold against cyber attacks one year, and the next year they slide back.a server level, must be able to detect whether a device has been jailbroken or rooted, then trigger a mechanism that prevents all enterprise-installed apps from running.

2014's big cyber chill

Financially motivated breaches aren't all that continued to make their mark this year. International espionage-related hacking remained big in the headlines. Notably, the US government took unprecedented action in May when a Pennsylvania grand jury indicted five members of the Chinese military on felony hacking charges.

While largely lauded as a bold step, not everyone cheered the move. "This is probably the worst thing we could have done," said retired Lt. Col. William Hagestad II, author of the book Operation Middle Kingdom: China's Use of Computers & Networks as a Weapon System, in our story published earlier this year. "When we place them on the same wanted posters as jihadists and terrorists, we say that we don't understand them and are out of ideas. And if there was any relationship building in place, it was castrated with this dumb action," he said.

The result of that indictment played heavily, Hagestad contended, into the chilling of the trade ties between the US and China this year. Audi, GM, Volkswagen, and companies in the tech sector "are all now being investigated for fraud or malfeasance because of that [indictment] action," he said.

Executives take notice

The cybersecurity headlines and data breaches are having an impact on perceptions of security by executives. "Especially when executives see the fallout at the executive level," says Kenneth Swick, information security officer at Citi Group. "I am seeing higher budget allocations, and from the additional recruitment activity across industries I am absolutely certain that financial sectors are responding to all of this breach news."

All of this makes the previous optimistic cybersecurity convictions in last year's Global State of Information Security

ADDITIONAL READING

Survey annual survey, covered in our story "Security spending continues to run a step behind the threats," look overly hopeful in comparison. In last year's survey, a surprising 84 percent of CEOs and 82 percent of CIOs stated that they believed that their cybersecurity programs were currently effective. Even 78 percent of CISOs expressed confidence in their programs.

An infrastructure remains at risk, breach incidents and costs rise

It seems that the very applications that help to keep the Internet secure and running revealed a number of deep crinkles this year. In April, a significant security flaw dubbed "Heartbleed" became publicly known. The flaw resides within the OpenSSL cryptography library and makes it possible to steal data from vulnerable systems. That flaw was shortly followed in September by Shellshock, another large vulnerability. Shellshock, a set of flaws uncovered in the popular Unix Bash shell, makes it possible for attackers to execute commands of their choice on target systems. Another flaw, POODLE, resides within the dated SSL 3.0 protocol, and makes it easier to steal user cookies and then potentially use that advantage to conduct further attacks.

The relentless hammering of new software vulnerabilities, the increasing sophistication of attackers, and misplaced optimism from previous years are all taking their toll. The reality is that more enterprises saw even more encroachments onto their networks, with the number of detected incidents rising to 42.8 million this year. That's an increase of nearly 50 percent from the prior year. In fact, since 2009, the annual growth rate of detected incidents has risen 66 percent.

For larger enterprises, the financial losses associated with these incidents are also up. Large companies experienced a rise of 53 percent in related costs. Mike Rothman, an analyst at the IT security research firm Securosis, says the rise in costs largely come down to regulatory mandated expenses associated with breaches – and larger enterprises tend to have many more records compromised than their small and midsized counterparts. Midsized organizations experienced a slower, but still a sizable, bump with a 25 percent increase in incident costs.

Security budgets flat, security analytics hot

Remarkably, IT security budgets are flat, even down in some areas, this past year. That result is causing some scratching of heads. "The drop in budget may not be an actual drop in real dollars, but an accounting shift," says Javvad Malik, an analyst at the 451 Group. That accounting shift could be related to enterprise refresh cycles, which would make the dip a temporary blip, or it could be due to the lower costs associated with cloud, virtualization, and employees increasingly bringing their own devices. "That's going be the long tail that's going to carry on for a number of years. We've seen a lot of investments move away from on-premise, and overall you may see a broad reduction of IT budgets," Malik says.

Brian Honan, CEO at Dublin, Ireland-based BH Consulting, agrees. "A greater adoption of cloud computing for enterprise applications and projects is the first reason," Honan says. "This is moving many large IT projects away from being solely IT budget items to items shared with business units," he says.

But data need to be comprehended to be useful. "The issue is not how much data you are getting, or how you look at data in new ways, but how effective is the information you get and how can you act on it? Pretty visualizations and pie charts don't protect your systems. Good actionable information does," says Honan.

One thing is certain: as more data is spread through on-premise clouds, mobile devices, and third-party providers, CISOs are going to need all of the information about how their data are being used, who is accessing them, and where they're going as they can get their hands on.

The rush to data-driven security

Perhaps the rising costs of breaches, the increasingly high profile of information security, and better insight from security-related data will have a positive impact on how enterprises successfully defend and respond in the years ahead. Many certainly are pinning more on increased insight through data. This year (the first time the survey question was asked), 64 percent of respondents reported that they use big data analytics to improve their security programs. And for those that do use big data analytics, 55 percent said that it can help in detecting incidents.

Malik isn't convinced that those results are reflective of the real-world use of big data analytics – certainly not as it's broadly defined. It's clear, however, that businesses of all sizes are using data more. They are reading their logs more. They are turning to their security information and even monitoring tools, and they're looking at the data they are collecting in a more intelligent way.

Given that broad definition of security analytics, it's accurate to contend that anything from basic log analysis to intrusion-detec-

ADDITIONAL READING

tion event alerts and up through sophisticated big data analytics fall under the umbrella of "security analytics" by many. Yet, Rothman argues that most enterprises heading down this path have yet to reach a level of maturity where their security data analytics efforts are improving their operational effectiveness. "I just don't think that many of these companies have figured out how to leverage those data more effectively. But they are certainly trying. That is clearly an area of increased investment in the industry," says Rothman.

Doing data right

How do enterprises do better with data? The solutions are straightforward, but not necessarily simple. "There are two approaches to figuring out what is happening in your environment. One is threat modeling. You determine what your valuable data are to potential adversaries. Determine the ways those adversaries could potentially get to those data. When that's complete, build a threat model around it and enumerate the monitoring analytics that are in place to look for those specific attacks," says Rothman.

The other approach is to baseline enterprise activity. There are tons of security-rich data within traffic logs and netflows; there are application and database logs; there are transaction data; there are authentication and logon data. Baseline these data, Rothman advises. "Then constantly look for anomalous situations that deviate from that baseline." But it's not just about raw data collection, of course. "The issue is not how much data you are getting, or how you look at them in new ways, but how effective is the information you get and how can you act on it? Pretty visualizations and pie-charts don't protect your systems; good actionable information does," says Honan.

Most of the experts interviewed suggest that enterprises also continue to expand the systems and types of data monitored. "If you are only using events from a certain type of device, start adding more events. If you are not using full back-capture, then start doing that. If you are not pulling end-point level telemetry, then that would be another area to start thinking about," says Rothman. "What you want to do is start building out a broader collection environment. This will give you the ability to start looking for patterns based upon a more inclusive and broader data set," he says.

Regardless of the level of enterprise maturity with security analytics efforts now, security technologies will have analytics capabilities built in soon. Gartner predicts that by 2020, 40 percent of enterprises will have built a purpose-built security data warehouse. "By storing and analyzing the data over time, and by incorporating context and including outside threat and community intelligence, patterns of "normal" can be established and data analytics can be used to identify when meaningful deviations from normal have occurred, the research firm predicted earlier this year.

That type of data analytics integration with security platforms would certainly be welcome. Perhaps that pervasive availability of security analytical tools will help solve what Citi's Swick says is one of the biggest challenges security pros have when it comes to having too much data with too little actionable insight. "Many CISOs are implementing SIEMs because that's what they're supposed to do. They don't understand enough about what it is that they are undertaking," says Swick.

Improved analytics toolsets could certainly help security teams to not only understand more about the data they collect – and the risks that events actually pose to the business – but also what to do about pressing threats and attacks much more swiftly than they do today. That most certainly would be a big and welcome step forward.