ENTERPRISE SECURITY FUNDAMENTALS

11/13/2019

Manel Ogal

Table of Contents

Overview

The current cybersecurity landscape is complex. Attackers develop new and ingenious methods of compromising systems on a daily basis. Intrusion tools, originally developed by the intelligence agencies of nation states, have been leaked, reverse engineered, and then made available to anyone clever enough to know where to look for them. New credential breaches are published on breach notification services, such as haveIbeenpwned.com, every few days. Exploit frameworks are updated to leverage newly discovered vulnerabilities.

Every month a new set of vulnerabilities is patched by vendors. Security researchers continue to find vulnerabilities in applications, products, and operating systems. Often vendors are able to release updates before knowledge of those vulnerabilities makes it to the public. While vendors are usually diligent in releasing updates to address vulnerabilities, information security personnel don't always get around to installing those updates in a timely manner.

In the current cybersecurity landscape, attackers are finding it simpler to monetize their activities, either by deploying ransomware that encrypts a target's data and system and demanding payment for a solution, or by deploying coin mining software that generates cryptocurrency using the resources of the target organization's infrastructure. Making a profit by compromising a target's infrastructure is becoming easier. This is likely to lead to a more, rather than less, aggressive cybersecurity landscape.

The current cybersecurity landscape is vast and likely impossible for any one individual to comprehend in its entirety. There are, however, several aspects of that landscape to which those interested in the fundamentals of enterprise security should pay attention. These include, but are not limited to:

- Technology lag
- Application development security
- Skill gap
- Asymmetry of attack and defense
- Increasing availability and sophistication of attack tools
- Monetization of malware

- Automation of Detection
- Internet of Things
- Transition to the cloud
- Increasing regulation

So one of the things we know about ransomware is that organizations know what ransomware is know that it's a threat and have actually taken preventative measures to deal with it. Obviously not all effectively but even with a fairly good backup and recovery strategy sometimes there's some files that you know you lose

It’s usually the organizations running outdated or unsupported products that you hear about when a large cybersecurity incident occurs. For example, the 2017 WannaCry ransomware attack disproportionally impacted organizations that had servers running the Windows Server 2003 operating system where the ports that are used for SMB storage protocol were exposed to the internet.

Application development security

The adoption of secure application development practices is another important part of the cybersecurity landscape. Many application developers create applications that are subject to attacks including cross-site scripting (XSS) and SQL injection, even though these attack vectors have been known about and understood for many years. As applications move from being locally installed on computers and devices to running as web applications in the cloud, it is important for organizations to ensure that secure application development practices are followed.

Skill gap

It’s regularly reported that the field of information security doesn’t have enough trained personnel to meet industry needs. The recent Global Information and Security Workforce Study by the Center for Cyber Safety and Education projected a global shortfall of 1.8 million information security workers by 2022. Organizations cannot begin to protect themselves from the various threats that exist, if they aren’t able to hire the personnel to manage and secure their information systems.

As you will be reminded throughout this course, information security is an ongoing process. It’s not enough to have a consultant come in, deploy, and configure software and hardware, and then your organization's information systems are secure going forward. Instead, the process of securing information systems is ongoing. For most organizations this means having IT staff that are trained in information security processes. Until the skill gap is closed, the cybersecurity landscape will be littered with organizations who are unable to substantively improve their security posture because they don't have access to the personnel that would enable them to do so and existing personnel are overworked due to a shortage of filled headcount.

Availability and sophistication of attack tools

While sophisticated attack tools are available often for free, there is a paucity of similar tools available for defenders. While the process of launching a basic or even moderately complex attack against an organization's information systems may be as simple as a mouse click, the defender's process of securing the configuration of those information systems is manual, complex, lengthy, ongoing and requires a good deal of expertise.

if an organization is diligent and applies consistent effort to its security posture, it will be able to protect its information systems against the common attacker.

The unfortunate reality is that even when organizations have highly skilled personnel, those personnel are rarely given the necessary amount of time and resources to ensure that the organization's information systems are configured in the most secure manner possible. The existing problem of asymmetry between attacker and defender is made worse by organizations not giving their defenders the resources they need to do their job.

Monetization of malware

A big change in the recent cybersecurity landscape is coin mining software. Coin minding software is software that mines cryptocurrency, such as Monero, Bitcoin, or Ethereum. This is a big change because in the past it was difficult for an attacker to monetize an intrusion. Coin mining software makes monetizing intrusions straightforward. An attacker who successfully deploys coin mining software on a target organization's information system just has to sit back and wait for the cryptocurrency to start rolling in. it's not unreasonable to assume that amateurs will be even more motivated to attack information systems in the hope of generating income.

Internet of Things

Another big change in the cybersecurity landscape over the past decade has been the rise of the Internet of Things (IoT). The IoT. is the network of physical objects, devices, televisions, refrigerators, home climate systems, cars, and other items, that are increasingly embedded with electronics, software, sensors and network connectivity that enables these objects to collect and exchange data. the operating systems of Internet of Things devices rarely receive long term security update support from their vendors.

The IoT presents an ongoing challenge on the cybersecurity landscape in that these devices are likely to remain insecure. This is because even when vendors do provide updates, unless those updates are installed automatically, few owners of these devices will bother to apply those updates. While people will apply software updates to their computers and phones when reminded, most are less diligent when it comes to applying software updates to their refrigerator, washing machine, or television.

How does this impact the cybersecurity landscape? Botnets, comprised of IoT devices have already been used to perform distributed denial of service attacks. While the processing capability of IoT devices is much less significant than that of desktop computers or servers, it's likely only a matter of time before an enterprising attacker works out how to get rich using a botnet of refrigerators to mine cryptocurrency.

Transition to the cloud

The cybersecurity landscape has been substantially altered by organizations moving on-premise workloads to the cloud. Important to note though is that moving infrastructure, applications, and data to the cloud doesn't mean that the responsibility for information security shifts from organizational personnel to the cloud provider.

As has been amply demonstrated by developers leaving cloud storage containers globally accessible, the security of a deployment in the cloud is as only as good as it is configured by the cloud tenant to be. Just as with on-premise information system security, the settings to secure workloads are present, but they must actually be configured by the information technology professionals responsible for those workloads.

For example, a cloud storage container used by a major US newspaper to host website code allowed read access to anyone in the world. Attackers used this access to inject coin mining code into the web pages delivered by the newspaper to its readers. Each time a reader visited the newspaper website, some cycles of their computer's CPU worked on generating cryptocurrency for the attackers who had modified the contents of the cloud storage container.

Overview

In the best of all worlds our organization's information systems are in a pristine state when we start implementing security controls. In this model, intrusions are something that exist as a future possibility rather than something that may have happened before you started thinking about how to secure your organization's information systems.

The assume compromise philosophy takes the position that an organization should build and maintain its security posture based on the idea that the organization's information systems have already been compromised. Another part of the assume compromise philosophy is that the organization should assume that preventative technologies such as firewalls, anti-virus, and intrusion detection systems (IDS) will fail. Under the assume compromise philosophy, information security teams focus instead on detecting and responding to suspicious activity rather than simply preventing intrusion. Detection of suspicious activity can be assisted by leveraging cloud-based analytics services that constantly monitor information systems telemetry for anomalies.

When you design a security posture with assume compromise in mind, you restrict an attacker's ability to move laterally between information systems and to restrict their ability to escalate privileges within those systems. These goals can be done by implementing technologies such as Just Enough Administration (JEA) and Just in Time (JIT) administration, segmenting networks, deploying code integrity policies as well as enforcing good administrative practices as restricting administrative sessions so that they can only be initiated from specially configured privileged access workstations.

Compromise examples

Few attackers compromise an organization without having an objective beyond proving that the organization can be compromised. Attackers target organizations because they wish to accomplish one or more goals. When an organization is compromised, the attackers often do one of the following:

- Exfiltrate data
- Deploy ransomware

- Enroll systems in a botnet
- Deploy coin mining software

Data exfiltration

The attackers extract sensitive data from the organization. This data may have been stolen for a variety of reasons, from the theft of commercially sensitive information to exposing organizational secrets to damage the organization's reputation. Some of the most famous attacks have involved data exfiltration, such as gaining access to a substantial number of customer credit card numbers.

Ransomware

In ransomware attacks, the attackers encrypt the organization's data and render the organization's information systems non-functional. The attackers do this in the hope that the organization will pay a ransom, usually in the form of a cryptocurrency. Once the target organization pays the ransom, the attackers will provide the organization with an unlock key. After inputting this key, the data will be decrypted and the information systems previously rendered non-functional will be returned to full functionality.

Botnets

Botnets are collections of computers that can be configured to perform a specific task, such as performing a distributed denial of service attacks. Botnets can be monetized in several ways, including extorting money through the performance of distributed denial of service attacks or used to relay spam (unsolicited commercial email).

Coin mining attacks

As of early 2018, coin mining attacks are becoming increasingly prevalent due to their lucrative nature. Coin mining malware deployed in attacks is sophisticated enough only to use some, not all, of the host systems resources, meaning it isn't always obvious when a system is infected. Coin mining attacks have also been perpetrated by insiders who use their organization's infrastructure to generate illicit income.

Systems rehabilitation

Once the attacker has been successfully ejected from the organization's information systems, it's then necessary to ensure that those systems are rehabilitated. Not only is it necessary to remediate the vulnerabilities that allowed the attacker to compromise the system, it is also necessary to ensure that any modifications that the attacker may have made to the system are located and removed. Rehabilitating a system isn't just a matter of reverting to the last backup as it may be that the attacker compromised the system some time ago. Reverting to the last backup won't remove the tools that the attacker placed on the system to retain persistence if those tools have been included in the system backups for some time. In many cases the only way to ensure that a system is rehabilitated is to deploy it again from the beginning and then address the vulnerabilities that allowed the attacker to gain access.

Reputational damage

Sometimes the biggest cost of a successful breach is to reputation. Reputational damage doesn't just occur when sensitive internal documents are leaked to the media. For example, consider an ecommerce site that suffers a breach where customer payment information is compromised. Customers of the site may be wary of using the site again in the future, especially if they've had to cancel an existing credit card as a result of the breach. When customers lose faith in an organization's ability to protect their information, they are less likely to interact with that organization.

Destruction of assets

Some attackers plant malware that is designed to destroy the systems of the target organization. Some malware works by reconfiguring hardware to work beyond its safe specification. For example, overclocking a processor until it overheats and fails. Other malware erases data on target systems or renders them inoperable. In some cases, the malware is deployed deliberately, destroying sensitive systems either to inflict financial damage or as a way of forcing the target organization's information systems to become inoperative.

Compliance costs

Another change in the cybersecurity landscape in recent years has been how regulation has encroached on the industry. Depending on the type of breach that occurs and the type of industry the target organization is in there may be fines that must be paid to specific authorities as well as investigations and reports that must be generated, all of which cost money and other organizational resources. In some cases, an organization that suffers a breach may be subject to ongoing reporting requirements for a period of several years. In some jurisdictions this can include paying for periodic external audits to ensure that the organization has correctly implemented the necessary security controls to minimize the chance of a similar breach occurring in future.