Implement and Operate End-Point Device Security Overview

Network security has two functions: to protect the network itself from compromise, and to protect the devices attached to the network from being attacked through the network. In this way, a network has two roles—the target of an attack, and the channel used in an attack. Network security should be a strong participant in the layered defense model that uses several layers of defense to protect assets of value, but relying solely on network defense to protect other assets such as data, processes, and applications from compromise is foolish. The attitude of the security practitioner should be to defend each device and each component of the systems and equipment of the organization from compromise. This includes the protection of each device that is connected to a network or even one that stands on its own but is supporting a business function.

Stand-alone Devices

Stand-alone devices are becoming rare as almost all devices now have network connectivity. An example of this is medical equipment in a hospital. Most of the monitoring devices and medical procedure equipment was once a stand-alone unit rolled to the patient's bedside and plugged into an electrical outlet. The medical staff would check on the device from time to time to notice if there were any alarms. Nowadays most of these devices can be plugged into the hospital's network and monitored from the nurses' station. This allows a medical professional to monitor many patients at once and receive any alerts in a timely manner; however, it also presents a new risk to the hospital, the patient, and the device itself. Most of these devices were built to be stand-alone units and did not have network-based security controls built into them. To network these devices now can result in another person or device being able to affect the operation of the newly networked device either intentionally or accidentally.

The risk with stand-alone devices is ensuring that they remain stand-alone or that they are built to be network secure in case they are connected to a network in the future.

A stand-alone device may also be subject to compromise by an administrator connecting to the device for maintenance. If an administrator connects with an infected laptop or carries a patch on an infected USB, it is possible that the device is now contaminated. This happened with STUXNET when it infected a stand-alone system that was air-gapped from the Internet through the actions of an engineer connecting an infected USB to the target system.

Thin Client

Early computer system users were often connected using a dumb terminal. These terminals had very limited functionality; therefore, they were quite secure. A user could not infect the core system because the terminal did not have Internet access of its own, and it did not have a CD-ROM or USB port that could be used to transport an attack. A thin client is a connected device that has limited storage capability.

This type of implementation has continued today with the use of thin client technology. A thin client presents very little functionality to the user and can prevent many types of malware or other infections that could otherwise occur through user misuse.

End-Point Device Security

The best approach to take to end-point device security is to assume and expect that the device will be attacked, or compromised—frequently and in many different ways. This attitude of paranoia can result in the wariness and caution needed to develop a secure end-point device security program.

Network-based defenses such as anti-virus, Data Loss Prevention (DLP), and firewalls are important, but they should be supported with the installation of such technologies on each end point as well. Each end point should be protected through a secure configuration and ensuring that all patches are kept up to date. This can require patching operating systems, applications, and utilities as well as upgrading firmware or other system components as needed. Typically, this is referred to as 'hardening.' This is especially a challenge, however, for systems that are part of the Internet of Things (IoT) since many of these devices will not be part of a normal patch management routine or easy to access for firmware updates.

End-point device security also addresses physical security through asset management and tracking, and locking or securing devices to prevent theft or alteration. Passwords should be required to perform any operations or maintenance on the device.

IoT (Internet of Things)

The Internet of Things is defined as the interconnection through the Internet of computing and network devices in everyday objects (physical devices, vehicles, buildings, etc.). The Internet of Things is an example of the problem of functionality versus security. Many devices are now connecting to networks to communicate and for maintenance. However, many of these devices have no native security functionality; therefore, they are subject to breach or compromise. Recent Distributed Denial of Service (DDoS) attacks have used IoT devices such as IP cameras in peoples' homes or home wireless routers as part of a large botnet to host and participate in an attack. Since many IoT devices are also connecting to the Internet via a wireless router, a compromise of the IoT device may allow an attack against other devices that are using the same router. Many IoT systems will not be patched or updated like other computer equipment or applications, so any vulnerabilities they have will remain on the device and available to an attacker once identified.

A consumer should be wary about allowing an IoT device to connect to the Internet and possibly only enable that connectivity when it is definitely required.

SCADA

Supervisory Control and Data Acquisition systems (SCADA) are essential components of critical infrastructure today. These devices collect data (data acquisition) and allow remote monitoring (supervisory) of processes such as electrical power distribution, dams and waterways, and traffic, for example. Many of these systems were initially installed as stand-alone systems, or they were connected to the monitoring station using a leased private line that was relatively inaccessible for a hacker. Now these systems are being connected through the Internet, and this results in significant savings for the organization. Many of these devices will have a lifespan of 30 or more years, and many that are now being connected to the Internet were installed over 20 years ago. They were written using languages and protocols that do not have any native security, and many are not readily securable. As new devices are built and installed, it is essential that they are built to be secure and protected from attacks or compromise.

Industrial Control Systems (ICS)

Industrial control systems are used to control industrial processes such as manufacturing equipment, robotics, distribution, and packaging. These systems are being connected to the networks of organizations so that, for example, a sales system will automatically send cutting diagrams to a laser cutter that will then cut materials necessary for assembly. Such automation saves human mistakes and time; however, an error with the system can result in expensive downtime or lost work.

ICSs are sharing the same network as other organizational processes and data. This means that a denial of service attack or a compromise of the network may affect critical business operations. In the case of an ICS that is managing the movement of molten steel in a manufacturing plant, even a momentary outage could be both dangerous and expensive. Many of these ICSs are not built to withstand an attack—even a simple probe may knock them offline. Such systems need to be isolated where possible and secured to prevent compromise.

Summary

Most attacks against information systems are avoidable by following best practices and implementing basic controls. This is especially true in the world of end-point security. Most compromises are the result of misconfiguration, default passwords, or unpatched systems. Having an end-point security program in place can avoid many of these problems and result in secure reliable operations of IT systems and equipment.

Operate and Configure Cloud Security Overview

Cloud computing describes an infrastructure chosen by many organizations to provide IT services. Cloud computing refers to the rental of IT services that can be easily configured, deployed, and operated to provide development platforms, fully featured applications, and network-accessible data storage and processing.

Cloud computing is based on an IT service that has been in use for over forty years, (virtualization), but it has moved from the earlier models of a remote mainframe being used by major organizations to the modern model of remote data services available to everyone whether as an individual, a government, or large organization.

There are several different deployment models in use today and various types of services available from cloud service providers. An excellent reference that can be used to describe and define cloud computing is the NIST Special Publication 800-146 Cloud Computing Synopsis and Recommendations (www.csrc.nist.gov).

The core concept behind the cloud is flexibility. This allows organizations to configure cloud services according to their individual needs, and it allows cloud service providers to provide custom services for their clients. This flexibility can also mean that various cloud service providers can define the products and services they provide quite differently from the way other organizations provide service.

Cloud security is based on the same risks and controls as traditional IT security and has the same requirement for risk management, control selection, monitoring, and reporting.

NIST defines Cloud Computing as follows:[1]

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models

Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."

[1] NIST SP800-146 Used with permission.

Cloud Deployment Considerations

The decision to use cloud-based services is primarily a business decision and usually based on economics and convenience. By migrating to the cloud, an organization can realize several key benefits:

- Save up-front capital costs for infrastructure acquisition
- Reduce time to acquire and deploy new IT equipment
- Gain access to an expert team of IT professionals provided by the Cloud Service Provider
- Pay only for the services used (measured service) and not be subject to paying all year for adequate equipment to support peak demand
- Savings in infrastructure (facilities, power support, network access, air conditioning) by sharing the costs with other clients of the cloud
- Have backup and recovery options in case of system, network, or facility failure
- Use of lower cost end point devices with less functionality (perhaps just based on the use of a browser without requiring deployment of applications to the end point devices.

In the end, a cloud provider is still just a datacenter(s) with all of the risks of fire, flood, power outages, equipment failures, and employee challenges that any IT organization faces. The Cloud Service Provider may guarantee a certain level of availability, but this is not a guarantee that the services will actually be available—just a way to financially reimburse a client organization in case of an outage. The service levels that the Cloud Service Provider agrees to provide should be enforced through Service Level Agreements (SLAs).

Examples of Cloud-based Risks

There are several risks associated with a cloud deployment. These cloud-based risks are in addition to the usual risks associated with an IT deployment and the development of an in-house security strategy.

Network Access

The use of cloud services relies heavily on high levels of network access. In all cases except perhaps a private cloud, network failure could disable all cloud functionality. Since the network is often provided by a third party (a telecom company), even the cloud provider has limited ability to ensure 100% network access. The cloud provider may have redundant connections, but this does not guarantee 100% access.

Transborder Data Flow

Many countries have laws that restrict the flow of data into or out of their country, especially [sensitive] data on their citizens. The use of a cloud provider may result in data being stored, processed, or accessed by personnel located in another country. It must be remembered that the organization that accepts the data initially is usually held responsible for ensuring the continuous protection of the data even if the data is passed to a third party for data storage or processing.

Cloud Service Provider Personnel

The personnel of the Cloud Service Provider will have the ability to access data on networks and systems they manage. This could lead to a compromise of an organization’s data if an unethical employee of the Cloud Service Provider mishandles data. Some organizations will choose to encrypt all data they store on the Cloud Provider’s systems; however, in some deployments (e.g., Software as a Service (SaaS)) this may not be a viable option.

Multi-tenancy

The Cloud Service Provider will often sell services to multiple clients. The data of each client should be kept separate from other clients; however, there is still the chance that data from one organization may be accessible to a competing organization.

Discarding Old Equipment

As equipment ages or fails, the Cloud Service Provider must replace that equipment. Since the discarded equipment may contain sensitive data, the Cloud Service Provider must have a secure procedure for discarding old equipment (degaussing).

Migration from the Cloud Service Provider

If an organization has been using the services of one Cloud Service Provider and then decides to move to another provider, there may be the risk that residual data is left on the backups or equipment of the original Cloud Service Provider.

Summary

For many organizations, the Cloud is their first choice for all new system deployments. The use of the Cloud may provide many advantages to the organization, but it also does come with a certain level of risk.

Implement and Operate Wireless Technologies Overview

The development of wireless technologies has allowed for a much more versatile workforce and enabled communications to remote areas not serviced by fiber or other cabling. There are many forms of wireless communications such as:

- Satellite
- Radio
- Wireless Local Area Networks (WLAN)
- Microwave
- Personal Area Networks (PAN)
- Bluetooth
- Wireless Metropolitan Area Networks

The security practitioner may work with several types of wireless technologies and should be aware of the risks and security controls needed for each type.

Satellite

Satellite technologies have enabled networking to nearly every part of the globe from mountain tops to oil platforms far out at sea. Satellite is a line-of-sight technology. The ground station must have a direct line of site to the satellite to be able to transmit or receive. The signal could be blocked by anything that breaks that line of sight such as heavy rain or snow, buildings or other large objects. The signal from a satellite can also be captured in many locations since the signal from the satellite has a large 'footprint' of area that can receive the signal. This requires the protection of the data from disclosure using encryption. Atmospheric conditions, such as solar flares, can also affect satellite communications.

Microwave

A microwave signal is also a line-of-sight technology. Microwave is used for transmission of communications across Earth, using towers that can transmit the signal from point to point across the network. Towers must also have a clear line of sight without interference from trees, high winds, or other obstacles. Microwave is used for local Internet access or long distance Wide Area Networks.

Personal Area Networks (PANs)

A network is defined as two devices that can communicate, and many people are the simplest of networks—a personal area network (PAN). It is common to use Bluetooth (based on the IEEE 802.15 standard) for enabling communications between a headset and a phone or other device. Bluetooth was designed to support short-range networks up to 10 meters (33 feet) in length. Bluetooth uses Frequency Hopping Spread Spectrum (FHSS) to overcome the noise and other interference that could otherwise affect communications on the congested 2.4 GHz frequency band.

Bluetooth

Bluetooth communications are subject to attacks such as jamming, which can cause a denial of service by flooding the communications channels with spurious RF (radio frequency) signals. Other Bluetooth related attacks include:

Bluejacking

> high jacking a phone through its Bluetooth connection and making calls from the phone

Bluesnarfing

> stealing data from a Bluetooth enabled device over the Bluetooth connection

Bluebugging

> listening into communications being transmitted via Bluetooth

Wireless Local Area Networks (WLANs)

Wireless LANs have had a significant impact on network architecture and business support. Most WLANs are based on the IEEE 802.11 standard. There are many implementations of the 802.11 standard operating in either the 2.4 GHz or 5GHz bandwidths.

Early WLAN implementations (e.g., 802.11b) were based on the WEP (Wired Equivalent Privacy) protocol and operated at nominal speeds of 11MB/s. WEP used the RC4 stream-based cryptographic algorithm with a short, 24 bit, Initialization Vector (IV). This proved to be fairly simple to crack and, therefore, provided an inadequate level of security. 802.11b also used a transmission method known as DSSS (Direct Sequence Spread Spectrum) to broadcast the signal.

Once the weakness in WEP had been discovered, the WPA (Wi-Fi Protected Access) standard was developed for secure wireless communications. This also improved the integrity of wireless communications by using a Message Integrity Code called “Michael.” WPA was still based on the RC4 algorithm.

The current standard for secure wireless communications is WPA2. It uses the Advanced Encryption Standard (AES) algorithm in a combination of Cipher Block Chaining (CBC) and Counter (CTR) mode. This is known as AES-CCMP for Counter Cipher Block Chaining Message Authentication Code Protocol.

Other transmission methods were also developed that overcame the limitations of DSSS. These included Orthogonal Frequency Division Multiplexing (OFDM) and MIMO (Multiple Input Multiple Output). The effect of these developments and the introduction of new standards, such as 802.11a, 802.11g, 802.11ac etc., has resulted in wireless transmission speeds that exceed 500MB/s.

Wireless devices present a serious security risk to an organization if they are not properly installed and configured. Some of the security controls used in the past, such as MAC filtering (where only devices that had pre-registered their Media Access Control (MAC) address would be allowed to connect to the wireless access point) or disabling the Service Set Identifier (SSID) broadcast, have proven to be inadequate to protect systems. Security administrators today use WPA2, along with a secure network architecture (isolation) and Radio Frequency (RF) management to protect against compromise of a network.

Some of the tools available to secure wireless networks include intrusion detection and intrusion prevention systems that can log and block suspicious network traffic. Wireless systems may also be implemented using Network Access Control (NAC) systems (based on protocols such as 802.1x) that will prohibit network access to a network unless the user is properly authenticated.

Wireless sniffing tools can capture all the traffic on a wireless network. The captured traffic can be analyzed leading to information disclosure.

WiMAX

Wireless Metropolitan Area Networks are based on the IEEE802.16 standard. WiMAX was developed to enable connected cities where everyone could have Internet access. The advantage of WiMAX over microwave was that it did not require line of sight.

There are several cities that have deployed WiMAX, but whether it really continues to be rolled out is doubtful because of competition from 4G, LTE, and other Mobile phone standards.

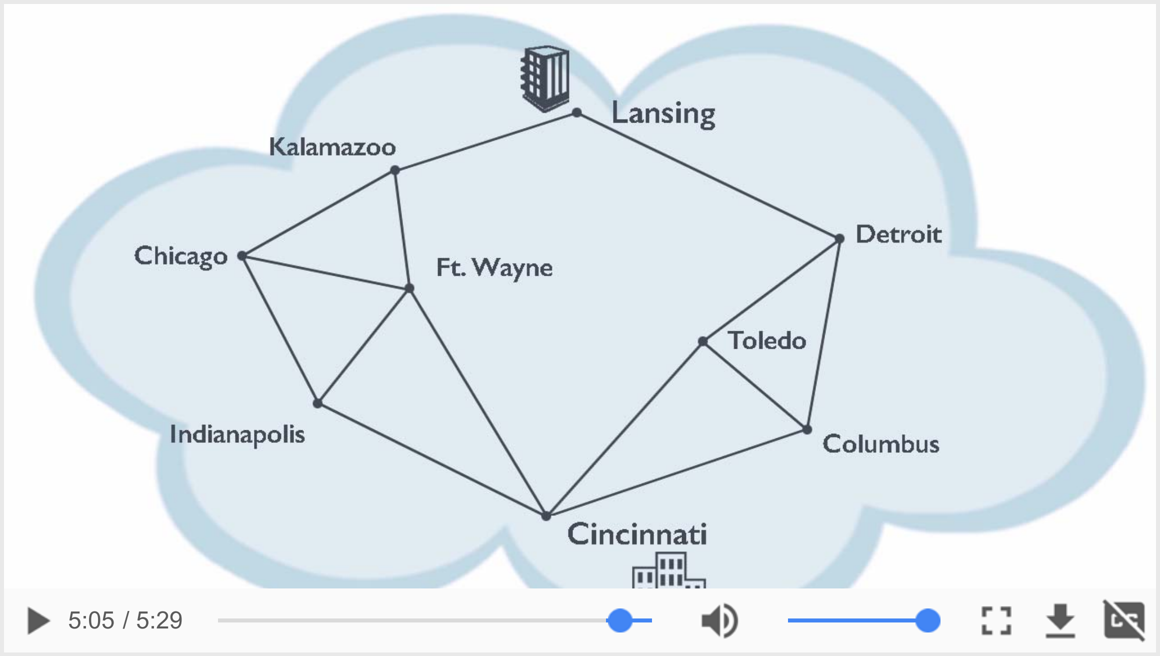
Summary

Wireless communications are commonly used in many organizations. There are some security risks associated with wireless; however, it is possible to deploy these technologies in a way that meets the security needs of the organization.

POTS and PBX Overview

The original telephone system used circuit-based communications by transmitting an analog signal over a low voltage (48vDC) battery-powered connection. The earliest phone systems established connections between the two calling parties (subscribers) by asking an operator to establish the connection. The operator would plug a cord into the phone line that ran to the called party's phone. The development of direct dial lines removed the requirement for an operator to establish the call and instead the rotation of the phone dial would cause a switch in the telephone company's central office to move and connect to the recipient. Every subscriber had a cable connection that ran from his or her phone to a piece of equipment in the central office. This was known as the subscriber line or last mile. In this way, the phone system was very much hardware based—each phone number was literally associated with a piece of equipment in the local central office. If a subscriber moved to another town, then they had to get a new phone number in the central office located in the new town. This was known as POTS, or the Plain Old Telephone System. It is also common to hear it referred to as the Publicly Switched Telephone Network or PSTN.

Establishing a phone call created a physical connection through whatever route was the best available at the time the call was established. Even if a shorter route became available after the call was established, the call would remain connected via the route chosen at the time the call was initiated.



▼ Transcript

Let's take a little look at the difference between circuit and packet switching. Circuit switching has been used for many years. Let's say we're gonna send traffic from Cincinnati, Ohio to Lansing, Michigan. There's a number of different routes or highways that traffic can take. We set up a circuit that will remain established for the duration of the conversation. With the old, plain old telephone system or POTS as we used to call it, this is how we set up our initial connection. Let's say that at the time when this connection was set up the best route available was actually from Cincinnati up through Indianapolis through Chicago, Kalamazoo, and onto Lansing. Once that circuit had been established, it remained established, and all of our traffic would flow over that route. Even if a shorter route became available, no we only establish the route at the beginning of the conversation. This allowed several very good benefits. With circuit switching, we would have a consistent amount of latency or delay in the processing. All traffic hit the same traffic problems and therefore was received in the correct sequence but also with pretty much the same amount of delay or latency. One of the other things that that did was it tended to eliminate jitter. And jitter is the variation in a rival times of packets where sometimes traffic will come very quickly but other times quite slowly. We could understand for a streaming media like voice, having jitter or having a variation in the rival times of packets could actually be quite annoying. With a circuit, we had a consistent level or a consistent quality of service all the way through the conversation. However, circuit switching can tend to be very inefficient as well. Instead, we found that if that road sat there through the night and nobody was using it, it still sat there and we paid for it. So, there's a lot of talk about instead moving towards packet switching. The idea let's treat this whole world as if it's one large cloud so that all of these switches are interconnected. When I need to send traffic from my head office here in Cincinnati up to maybe a branch office in Lansing, then I would break my traffic into individual packets or individual pieces. And, they would find their way across this cloud of switches to whichever route was the best available at that time. We would take the entire communication, break it into manageable-size pieces, address each one. The same as if we took a textbook and wanted to send it through the mail 10 pages at a time. We would take the first 10 pages, put them into an envelope, address it, and then mail it off. And that packet would route through the network, whatever was the best route available at the time towards its destination. The second envelope could actually take a different route up through Toledo and Detroit. The third might take a different route as well. After Toledo across to Ft. Wayne and then up through Kalamazoo to Lansing. What do we have? We now have a variation in the arrival times, and we have a difference in latency or the amount of time taken for packets to get to their destination. And, sometimes out of order, packets in sequence would come. The problem was we needed to reassemble the packets into the correct order. We had to deal with a little bit more jitter or variation in arrival times. But this meant that all of our networks could be used much more efficiently. Whichever road was available was the one that was used. It also meant that if we had a breakdown say of one piece of highway, traffic could easily route around that towards it's destination. So, some of the principles of going to packet switching were very much suited towards data. Data tends to be bursty. It tends to be communicated in clumps or chunks of data rather than in a stream of data. So, packet switching work incredibly well in a databased environment. And of course most of our communications today, even using voiceover IP, are using packet switching technologies.

Circuit switching was excellent for voice communications since the quality of the communications remained consistent throughout the call. The latency or delay in traffic flow was consistent and there was no jitter. Jitter being the variation in transmission speeds that is so typical with packet switching (data networks). This also meant that all the traffic was sent over the same channel in the same sequence. With packet switching, packets may arrive out of order and at various speeds.

PBX

Some businesses would have their own telephone switch known as a Private Branch Exchange or (PBX). This switch managed the calls within the organization by assigning a port (an extension number) to each phone. Calls could then be routed to individual phone extensions by the switchboard operator. This led to considerable amounts of telephone fraud, since a thief could dial into a misconfigured PBX and then enter a code to get local dial tone. This enabled the thief to be able to make calls anywhere in the world and have them billed to the organization that had a PBX.

Attacks

The hacking community that focuses on telephone fraud is known as "phreakers". They publish a magazine called 2600 that describes how to exploit telephone vulnerabilities. 2600 hertz is the signaling frequency used to control some telephone operations and by exploiting this frequency, the phreaker could make calls for free and sell those services to other people.

The greatest risks to the POTS were cut cables (construction work), equipment failure, and loss of commercial power. Almost all phone system equipment is duplicated to provide for redundancy and failover, and backup batteries and generators provide power in case of a power failure.

Computer Communications

The development of computers and the need to enable them to communicate over phone networks brought new challenges to the POTS. The phone system was the natural method to enable computer-based communications. This area has evolved tremendously over the past few decades.

Analog signals vary by frequency and amplitude and, like the human voice, vary in volume (amplitude—the strength of the signal) and pitch (frequency—whether a high frequency squeak or a low frequency growl). As a person speaks over a phone line, their voice is transmitted as an analog signal. At times the phone cable may have some noise but in most cases that was acceptable, and the parties could communicate effectively over that noise (static). As the signal is transmitted down the cable, it begins to lose its strength through attenuation. Eventually the amplitude would be so low that the voice could not be heard. This required the installation of an amplifier to boost the strength of the signal. However it could be difficult for an amplifier to know the difference between a voice pattern and any static, so it may boost the static as well.

Digital signals are a series of pulses of electrical current (copper cabling or microwave), or light (fiber optic cables). Over distance these also attenuate and need to be regenerated through a repeater. The advantage of a repeater is that it generates an entirely new pulse, it does not just strengthen the existing pulse. This allows a digital signal to remove noise or detect errors on the line.

MODEMS

Computers speak digital whereas the old voice-based telephone system was analog. This meant that a modem (modulate/demodulate) was needed to covert the digital signal from a computer into an analog signal that could be transmitted over the traditional phone system and then convert it back into a digital signal at the receiving end. The challenge was that data signals cannot tolerate noise or interference, and the old voice grade telephone cables often had some noise on them. This required the use of parity bits to detect errors in transmission.

When a user dialed into an ISP (Internet Service Provider) using a modem, the connection was established using Point-to-Point Protocol (PTP). An earlier protocol was SLIP (Serial Line Interface Protocol). The PTP connection was then used to authenticate the user using PAP (Password Authentication Protocol). PAP sent the login ID and password in cleartext, but this was an acceptable practice at the time since monitoring a telephone link is more difficult than monitoring a network connection. There are still some systems that use PAP today, but this should only be done over an encrypted tunnel.

Point-to-point protocol is still in use as well, but usually it is wrapped in a tunnel created using Point-to-Point Tunneling Protocol (PPTP). PPTP does not create an encrypted tunnel and requires additional encryption to be secure.

Leased Lines

When an organization needed to communicate between two computer systems on a frequent or continuous basis (such as between a branch office and a head office), then a modem was a slow and ineffective solution. The company would arrange with the phone company to provide a leased line that would be a private network for the company to use for its communications. The leased line was a dedicated circuit that could handle digital data communications. The price for such a line was based on the distance between the two end point computers—the company was charged monthly for such a circuit by the mile. In return this circuit was available exclusively for the company that paid for it and usually had some guarantees of availability. This private network was expensive and also somewhat inefficient since the customer paid for the circuit 24 hours per day even if they only used it for a fraction of that time.

X.25, Frame Relay, and ATM

The next step in data communications was for the telephone company to set up a cloud of data switches in each central office and then lease access to that cloud to companies that needed data communications. The client companies purchased a point of presence on the cloud and could transmit data across this shared network of switches. This resulted in a significant cost savings for the company since the users of the service share the cost of the network and each company only pays for the amount of data they transmit. It also improved the efficiency of the network since many companies can share the same network routes.

One of the earliest data packet switching technologies was X.25. This service could only handle data (as compared to later services that could handle multiple forms of communication). X.25 was built for poor quality, voice grade communications so it did error correcting at each step along the transmission path.

At the Datalink layer of the OSI stack, the packet of data being transmitted is known as a “frame.” The next major technology to be used was entitled Frame Relay and it was much faster than X.25. Since most of the major cables between central offices were now fiber optic cables, there was no need to do error correcting at each point.

Asynchronous Transfer Mode (ATM) divided all of the data into fixed sized cells to transmit them. It was an efficient way to communicate over a cloud of ATM data switches.

QoS and CoS

Quality of Service can mean two things: in the telephony world it usually refers to the quality of the transmission media, for example, availability, jitter, dropped packets, etc. But in the networking world, it can be used to set out prioritization of traffic. This is also known as Class of Service where higher priority traffic will be processed before lower priority traffic.

MPLS

MPLS or Multi Protocol Label Switching is a method of managing and engineering data communications. MPLS allows the customer to engineer the route their traffic will take and set priorities for certain types of traffic. This way, the company can know the route for their traffic and perhaps avoid certain risks and give higher priority traffic preference as it is transmitted.

Permanent Virtual Circuits (PVC)

The problem with using a packet switched network was the loss of control over the routing of the packets. Packets could route almost anywhere to get around congestion or network failure, which increased availability, but they could also end up being routed over a network belonging to another country, which may be a concern for data privacy. The packets could come out of order, which required buffering and reassembly at the receiving end. Because of these variations, some companies wanted to have a dedicated route that their traffic would take over a packet switched network. This routing is known as a Permanent Virtual Circuit (PVC). It makes a packet switched network operate similar to a circuit switched network. The PVC was a permanent route, and all the traffic from the company would travel over this route. Another option was to set up a Switched Virtual Circuit (SVC) where a “circuit” or route over the network would be established for each session according to what was the best route available at the time.

Software-based Telephony

By the 1970s the world of telephony was changing, and the new telephone switches in the central office would associate a phone number with a piece of equipment using software instead of the older method of a phone number being a hardware-based location. This was an important step in developing flexibility in telephony. Now a person could have a phone number from one town or central office that they could use in a different town or location. Today, a customer can even "port" a phone number between different telephone suppliers, and their mobile or cellular phone can be reached from almost anywhere in the world. The breaking out of hardware-based management to software-based management has created the environment we use today in software defined networking, content delivery networks, and many other applications.

This development revolutionized the world of telecommunications and introduced the world of today with Voice over Internet Protocol (VOIP) and Cellular (mobile) phone service.

Converged Networks

Data is data, and a data network can handle data of many different protocols. This has meant that organizations can deploy a single network that can handle voice and data traffic, instead of having separate networks. Many different types of data can be transmitted over the network including email, files, music, videos, and television. This convergence has led to the subscriber line to a customer’s home being used for voice, Internet, and television traffic simultaneously. This requires the subscriber line to be upgraded to a digital connection, hence the name Digital Subscriber Line or DSL. This upgrade requires the removal of any bridge taps (branches) on the cable and the installation of repeaters if the signal has to travel too far. Since a digital signal attenuates quite quickly, the maximum distance that most subscribers could be away from the central office was 18,000 feet or about 5 kilometers.

Converged networks allow a telephone company to sell many services over the network connection to a business or home. If the subscriber still has a normal analog telephone they use for voice, as well as an Internet connection running over the same cable, the telephone company would install a DSL Modem on the voice network in the subscriber’s premises to convert the voice call to a digital signal and a DSLAM (Digital Subscriber Line Access Multiplexer) in the central office to separate incoming voice packets from other data packets and route the voice onto the traditional PSTN.

VOIP

Voice over IP takes a voice conversation and converts it into a digital signal to be transmitted as data packets over a digital network. Converting an analog phone call into digital has been done for many years so that multiple conversations could be transmitted over the same cable at once (known as multiplexing). Multiplexing was traditionally done using Time Division Multiplexing (TDM), where each call would run on a separate channel and each channel had its own time slot, or Frequency Division Multiplexing (FDM), where each call would run at a different frequency— like the radio where each radio station broadcasts at a different frequency over the same medium (the air).

In many countries, the entire backbone used for telephony calls is already VOIP. The IP networks used for data communications carry the voice packets as well. There are many applications that use VOIP such as social media networks that allow a person to call over SKYPE® or WhatsApp. The advantage of VOIP calling is that it can be conducted at a fraction of the cost of traditional long distance phone calls.

Voice conversations are a type of streaming media that flows with data as a person speaks. If the conversation was broken into pieces and came as blocks of data at a time, the conversation would be difficult to tolerate and understand, like reading a sentence that came as pieces instead of as a stream. This means that the VOIP conversation should be able to flow at nearly the same speed as a person speaks and be able to recreate the conversation at the far end into a normal stream of conversation. If the network is too slow then the call becomes unmanageable and broken. VOIP requires, therefore, a decent network connection to work acceptably.

Packet Loss Concealment (PLC)

Undoubtedly when a VOIP conversation is ongoing, the occasional packet will be lost. With most data connections, the loss of the packet would be noticed and a new packet sent (TCP). However, with voice this would not be acceptable. To resend a lost packet a few seconds later would confuse the listener. They would hear a word that should have been earlier in the conversation. For this reason, the system will not try to resend a lost packet, instead, it will attempt to conceal it. When a person speaks normally, the occasional word may be lost, but since the listener hears the rest of the sentence they can guess what was said, and they do not have to ask the speaker to repeat what they said. However, if too much data is lost, then they do need to ask for the speaker to repeat. With VOIP, the system will just ignore a lost packet and hope the conversation can still be understood, or it will just duplicate (repeat) the previous packet, hoping that perhaps the lost packet was similar to the previous packet.

Cellular (Mobile) Phones

In North America, it is common to refer to cellular phones as cell phones, but in many other parts of the world, they are known as mobile phones. For the sake of clarity, this article will use the term cell or cellular phones.

The earliest cellular phones ran on an analog radio network and had very limited functionality and battery life. For the most part, they could only handle voice conversations.

There were several protocols used for cell services such as CDMA, TDMA, GSM, GPRS, HSPA, and LTE. Each protocol represented improvements in the way that cell services were offered and increased the functionality of a cell phone to be an always-on connected device. Today's smartphones are incredibly powerful small computers that can handle data and voice traffic at excellent speeds and allow seamless connectivity to a person travelling at high speed. The cell network is a series of cell towers that are arranged along the lines of cells or like a honeycomb. A person's cell phone can often connect to several towers at once, but it will select the tower with the strongest signal. As the person travels into range of another tower, an ongoing call should be "handed off" to the next tower. Ideally the customer will not even realize they are now linked to a different tower since the call is passed on with little or no interruption. This is an example of how one phone number can be associated with several different hardware devices within minutes.

The functionality and versatility of cellular phones has led to them replacing traditional landline phones in many places.

Secure Device Management

Many security breaches are the result of insecure or misconfigured end point devices. Especially as many devices are now being used for both business and personal use, the risk is compounded since a breach caused by personal use may affect business data. For this reason, an organization that allows BYOD (Bring Your Own Device—sometimes known as Bring Your Own Disaster) should have policies in place to govern the secure use of such devices. This may include the use of Mobile Device Management (MDM) software that can create an isolated environment for organizational data and allow the remote wiping of the device if it is lost or stolen. Organizations may also have policies in place that restrict what applications can be installed on a device through whitelisting.

The secure configuration of end point devices is critical to ensure the protection of the devices and the networks the devices are connected to. An insecure device such as a wireless router, smartphone, or laptop may lead to expensive and embarrassing breaches for an organization.

Secure device management includes hardening the device by disabling functionality that is not required and ensuring default passwords and administrator accounts are changed. Asset management will also track corporate assets and ensure they are accounted for on a regular basis.

Summary

Telephony and Networks are the foundation for almost all business operations today. Organizations must use wisdom in designing, implementing, and operating network devices to ensure reliable and secure operations.

Operate and Maintain Monitoring Systems Overview

This chapter addresses the concerns of Incident Management and the need to be prepared to handle the many issues and events that threaten business operations. The primary objective of a security program is to avoid or prevent interruptions to business services through the implementation of adequate controls. However, every organization will face numerous challenges and incidents that may even threaten the survival of the business.

The first requirement of incident management is to be aware of an incident as quickly as possible. It is not reasonable to expect that an organization can address a problem if they do not know about it, and numerous studies have shown that most organizations lack the monitoring and detection capabilities needed to be alerted to an incident in a timely manner.

The first part of this chapter will examine the monitoring and reporting functions necessary to detect and alert IT staff, security, and management about the current state of their systems, security, and risk. Later sections will examine the incident management process and how to manage a crisis in an effective manner.

Operate and Maintain Monitoring Systems (e.g., Continuous Monitoring)

An information security program is founded on the principles of risk management. The identification and assessment of risk leads to the selection of a risk response. In many cases, a risk will be addressed through the implementation of controls. Those controls may be managerial, technical, or physical. All three types of controls are necessary to ensure the effective mitigation of risk. A firewall, for example, will not be an effective control if it is not implemented correctly, supported by trained personnel, physically protected, and subject to monitoring. A technical control in itself is not sufficient and may even lead to a false sense of security (the old adage applies, “we have a firewall so we must be secure”).

Every control must be tested to ensure correct operation. This is where the monitoring and assessment of the control is important. There are three questions that should be addressed by control assessment:

1. Was the control implemented correctly?
2. Is the control operating correctly?
3. Is the control meeting its desired result (mitigating the risk)?

The review of the implementation of the control is the first step. Whether the control was purchased or created, the implementation should meet the design requirements of the control. It is common to find that the “as-built” (how the control is in real life) is substantially different from the intended design of the control. This may be necessary if the design was not feasible, but it may also be that the implementer cut some corners and tried to save time and money by not doing everything the design called for. If changes had to be made in the implementation of the control, then they should be subject to approval and properly documented, along with the justification for the changes.

It would seem that the next question, “Is the control operating correctly?” would be the final answer to the assessment question, however, that is not the case. A control may operate correctly—a firewall, for example, may block undesirable traffic and allow other traffic—but still not mitigate the risk. The firewall needs to be examined both from a configuration perspective that would examine its rules and security settings, as well as from a management perspective. The firewall needs to be managed by adequately trained staff, have change control procedures in place to manage rule changes, and have a person assigned to review the logs on a regular basis. All of these functions are necessary for the control to be operating correctly.

The third question takes us back to the risk that was used to justify the implementation of the control. A control should always be implemented in response to an identified risk. A control not associated with a known risk is almost certainly unnecessary and should be removed. A control impacts productivity, costs money to operate, and may annoy users especially if no one knows why the control is needed. The review of the risk that justified the control is essential to ensure that the control is the right control, that the control is addressing the risk, and that it is supporting business goals. If an access control system has been implemented, then the review of the control should include whether people can bypass the control and whether it is reliable and effective to prevent unauthorized access and permit authorized access. If it is found that users can bypass the control, then the risk should be examined to determine whether the control should be removed, strengthened, or replaced.

Monitoring Key Areas

When a person visits a doctor, the doctor will usually start by examining a few vital statistics such as blood pressure, pulse, and reflexes. That is because those are good indicators of overall health. However, if the doctor has cause for concern and believes the patient may be at risk then the areas examined are increased accordingly. The same concept applies to monitoring information systems controls. There are far too many logs and events created every day by multiple systems for any organization to monitor them all, so it is preferable to select a few of the more important controls for regular review.

Monitoring key areas can facilitate reporting and analysis of security events and allow management to be informed of risk without being overwhelmed with so much data that it is impossible to accurately measure the true condition of the security program.

Discussion: Key Areas

What are some key areas that should be examined and reported on?

☆ Review: Key Areas

The challenge is to determine the “right” areas to report on. This is often accomplished through communication with management. Learning what management is interested in and reporting on those areas is more likely to gain management support than to generate reports the recipient does not really care about.

The areas reported on may change over time as business priorities and risk changes, but delivering consistent reports that allow comparison between reporting periods will allow the detection of trends and patterns of activity that may require security administrator intervention.

Audit Planning

The traditional manner of reporting has followed the traditional structure of auditing. Auditing creates an audit plan at the beginning of the year that lists the areas subject to audit over the coming year. Audit resources are then assigned to perform the audits; however, there are rarely enough resources available to conduct all the audits that management would desire. Therefore, audit focuses on areas of higher risk and hopes to audit the other areas in the future. This can mean that an audit of an area may be conducted only once every few years. This is a rather ineffective way to alert management to a risk. A change in a process that has created a risk may happen shortly after an audit and then remain undetected on the system for several years before audit returns to find the risk.

Audits may be conducted by either internal or external parties. Internal audit is driven by management and reports to the management of the organization. Internal audit has the advantage of knowing the structure and mission of each department in the organization better than an external auditor would. But audit is only as good as the skill of the auditor and the independence of audit from management. An auditor that merely uses a tool and reports on the results of a checklist is not likely to provide any real value to the organization. An auditor that can interpret the results of the test and dig into any issues that are indicated can provide excellent value.

Audit Standards

Audits are conducted against standards. The standards used in the audit are the benchmarks that the processes of the organization are measured against. This provides credibility to the audit report. When an audit is performed against an internationally recognized standard, such as ISO27001, this provides management with a report on how the security profile of the organization compares with international best practice.

Compliance

In a world full of regulations and legislative mandates, an inordinate amount of security practitioner time is consumed with assessing and reporting on regulatory compliance. Part of the challenge is that many regulations do not document specific actions for compliance and non-compliance, and organizations struggle to interpret the requirements of the legislation. The security practitioner should work with security management and the legal department to ensure a correct understanding of regulations and be familiar with standards such as PCI-DSS that may require compliance. Failure to address compliance issues may result in financial or criminal charges against the organization and individuals.

Audit Reports

Audit reports are confidential documents that may expose some of the vulnerabilities in the organization. Therefore, audit reports should only be distributed according to the policy of the organization.

The auditor will often deliver a draft report to management first. This allows management to clarify assumptions, or correct any errors in the report, and to respond to the recommendations in the report. The final report is then issued to include the responses from management.

Continuous Monitoring

The problem with most security reporting and audit is the delay in identification and notification of an issue. An issue that arises in between reporting periods may not be detected until the next reporting period. This problem has led to the concept of continuous monitoring. Continuous monitoring should detect an issue in near real time and enable the response and mitigation process in a timely manner. The difference is that most security reporting is done by security management, and audits are done on an infrequent basis by auditors, while continuous monitoring is the responsibility of line (front line) managers. Managers are responsible for the actions of their staff and for ensuring their staff is following procedures and the policies of the organization. Managers are in the best place to immediately detect any areas of non-compliance or security issues. This is a culture shift for most managers that have considered the enforcement of security policy to be the responsibility of another department. With continuous monitoring, managers are expected to be monitoring for any abnormal conditions or incidents that may require attention, whether the issue related to staff, technology, communications, or procedures. Managers can then initiate the response process that will address the issue in a timely manner.

To move toward continuous monitoring requires the education of management in what to look for, what is normal/abnormal behavior, and how to report an issue. When a continuous monitoring process is in place, it may preclude the need for an in-depth audit, and a visit by the auditors may result in a very brief review and report on the status of the continuous monitoring process.

Sensors and Sensor Networks

One advantage the security practitioner has is the availability of many sources of data regarding systems, network, and user activity. These sources allow the collection and analysis of data about incidents or abnormal activity. Many sensors operate continuously and can immediately detect an incident and initiate an alert. These include firewalls (including Web Application Firewalls (WAFs), packet filtering routers, stateful inspection firewalls, and proxy devices), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), cameras, and motion sensors.

Physical

Physical sensors include motion and vibration sensors (infrared, fiber, light-beam) and cameras, security guards and dogs, and smoke detectors. The problem with a sensor is that it often requires a response from a knowledgeable person— one able to interpret the type and severity of the incident. Misreading or ignoring the alarm can result in an uncontrolled incident that may cause significant damage. As is often the case, the ability to catch an incident in its incipient (initial) phase may permit the containment and resolution of the incident before more damage occurs.

The problem with many sensors is the number of non-adversarial events that may trigger an alarm. These repeated "false" alarms may desensitize staff to the point that they ignore a real incident when it does happen. All sensors need to be maintained and monitored in order to provide a benefit.

SCADA and ICS

Supervisory Control and Data Acquisition Systems (SCADA) have been around for decades. These sensor networks monitor many parts of the critical infrastructure (electrical power distribution, for example). The problem is, in part, that these devices work very reliably and are often left in place for years without requiring updating or maintenance. The same risk also applies to Industrial Control Systems (ICS) that manage industrial processes (everything from movement of materials in a manufacturing operation to controlling robotics).

Originally many of these devices were isolated from the Internet and were not connected to any other devices besides the control station or network that was used exclusively to manage these systems. Now, more and more of these devices are being connected to networks and the Internet. However, the protocols used and design of these systems did not include the security functionality necessary to protect them from compromise. This is a problem as many more devices are connected to networks that were previously unconnected—the development of the “Internet of Things” or IoT. As many home and low-end commercial devices are network enabled, they are also subject to network-based attacks. The creation of large botnets of compromised IoT devices has led to some of the largest Distributed Denial of Service (DDoS) attacks seen to date.

Network Sensors

Network sensors have two areas of responsibility: to protect the network itself and to prevent the misuse of the network by malicious traffic. Network sensors may act as a gateway that enables or prohibits access such as a firewall, or they may monitor traffic for analysis such as a Network-based Intrusion Detection System (NIDS).

NIDS

A network-based intrusion detection system sits alongside a network and captures a network that passes by. It does not intercept or block traffic, and it only monitors traffic in a stealth mode. The IDS is limited in that it cannot take decisive action on an attack, it can only alert an administrator or other device to respond appropriately (reset the connection, drop future packets, etc.).

The challenge for the IDS is the inability to "see" encrypted traffic. This means that the ability of the IDS to effectively monitor traffic is impaired.

NIPS

A network intrusion prevention system actively intercepts and blocks network traffic that it considers undesirable. It operates in the middle of traffic stream and is able to respond in real time to malicious traffic. It can help protect the network segment it is installed on and may contribute alerts to devices on other parts of the network to protect them as well.

Again, the challenge for the IPS is the inability to effectively read encrypted network traffic.

Host-based Sensors

There are several types of sensors used on a host whether it is a laptop, server, or other end-point device. These sensors are often used to protect individual hosts and are then limited in their ability to protect other hosts. A host connected to an insecure network is subject to attack, and having effective prevention and detection tools on the host is imperative.

HIDS

A host-based IDS usually works on the basis of comparing the current state of the host to a previous known good state. This means that it will detect a change in a file or executable and alert the administrator to the change. This may identify a situation where a host file has been corrupted by an unauthorized change (perhaps by malware or a Trojan Horse).

The advantage of a host-based system is that it can see the activity once it has been decrypted. It is limited, however, in that it is too late in the process since the change has already been made.

HIPS

A host-based IPS can block an unauthorized process from making a change on a system. The HIPS will alert the administrator to a pending change and require the approval of the administrator before allowing the change. This is built into most operating systems today and is a valuable tool to alert a user to a program trying to make an unauthorized change on their system.

IDS and IPS Engines

IDS and IPS devices use the same approaches to analyzing suspicious activity. These approaches include pattern-based and signature matching algorithms and anomaly-based algorithms.

Pattern- and signature-based algorithms compare current activity against known types of attacks. Once the device has been told to watch for a suspicious signature, the device is very accurate at finding any such attacks. This means that such systems have a very low False Positive Rate. A false positive occurs when a device indicates an alarm (a positive result) when no real adverse event has occurred. On the other hand, such devices are subject to a higher false negative rate since they will not detect an attack unless they have been told to watch for it. This makes such devices ineffective against a new type of attack. A false negative is where the device has tested the traffic and indicated there is no problem even though malicious traffic was present. This is often considered more dangerous than a false positive since a false negative means the staff is not aware of a problem even though it exists. It is hard to address a problem if the problem has not even been identified.

Anomaly-based systems look for abnormal traffic flows or types. This requires the system to be aware of what legitimate (normal) traffic is. It is not really possible to detect an anomaly if no one knows what is normal.

Anomalies may include new types of traffic or an executable not seen on the network or device before, a flood of traffic that exceeds normal statistical traffic flows, or protocol anomalies that would detect a packet that does not fit in with its defined packet structure.

Heuristic scanners will divert a suspicious packet into a safe quarantine area. This area may be a “sandbox” environment that allows the packet to be examined without posing a risk to the rest of the system or network. The packet can then be dropped or forwarded depending on the results of the examination.

Application Logs

To use an analogy from the physical world, applications can be compared to the “roof” of a building. They are the primary target of rain, snow, sun, wind, and dust. A breach in the roof will often lead to damage to all areas of the building, and despite the strength of the walls and floors, everything is affected. Applications allow users to perform functions on our networks, systems, and data. This is especially dangerous when the majority of users of applications are untrusted people over the untrusted Internet. If an application is not adequately secure, then all of the data and systems of the organization may be vulnerable to attack.

To protect the data of the organization and ensure correct operation of the applications, it is essential to build the ability to log user and application activity into the applications. Logs should capture changes to data and record the identity of the user that made the change, the time of the change, and the type of change. Logs should also record details of application operation such as errors and transactions processed. These logs allow the administrator to trace any problems and identify the source of a transaction error.

Protecting Logs

Logs are essential to support business requirements. They should be enabled to capture and retain information as long as necessary for legal or business reasons. Because logs may be needed to prove compliance with regulations, assist in a forensic investigation, and track the source of an error, the logs must be protected from deletion or manipulation. Logs may also contain sensitive data about customers or users and should be protected from unauthorized disclosure.

The length of time to retain logs varies according to the importance of the data in the log and the mandates of laws that may require retention of log data for many years.

Protecting logs may be done by writing them off to a central location where all log data is securely kept. This prevents an administrator from deleting or altering the data in the logs if the logs were stored solely on their system.

Data Analysis

Logs may contain incredible amounts of information. This makes them unmanageable and impossible to handle through a manual process. The security practitioner must find the few items in the logs that are relevant and important in order to act on the log data appropriately. This almost certainly requires the use of log management tools that can filter and analyze the log data efficiently. The log management tools may allow the administrator to filter out certain types of events or set clipping levels where an event is only identified if it happens at a certain frequency. This is often done with a password, where a clipping level is set at the threshold between normal user error and a brute force attack. A user may enter their password several times incorrectly, but no action is taken until they have exceeded the threshold of three or four invalid attempts within a short time period. Once the threshold is crossed, the account is locked out. Log data may be analyzed in the same way so that only when a certain activity happens more than a certain number of times will the event be recorded or identified.

The security practitioner may also record activity on a network using a tool such as WireShark to capture wireless network traffic. This tool allows the practitioner to see network traffic and detect any activity that requires further analysis.

SIEM

Security Information and Event Management systems are one of the primary tools used for log and event correlation and analysis today. They collect data that has been captured by multiple devices and bring it together for analysis. From the data analysis, a SIEM generates reports used to indicate the overall health of an organization’s security program. This is a valuable tool for management. The SIEM also operates in near real time and alerts to unauthorized activity, allowing the administrators to take action in a timely manner.

By correlating data from many disparate sources across the organization, the SIEM is able to create visibility into events and link activity at one location with activity at another location.

The challenge with a SIEM is to develop the analysis skills necessary to manage the data and tool effectively. Without the skilled staff to configure, analyze, and interpret the results generated by the SIEM, the SIEM can become little more than a very expensive report generator.

Summary

Log analysis is an essential part of a security program. Without the ability to test systems and assess the results of system and network activity, the security practitioner is unable to effectively evaluate the security program. A lack of monitoring and reporting also means that management is not going to be able to execute their responsibilities in providing IT governance and assurance of compliance.