**Organizational Network Security and**

**Intrusion Detection and Prevention Systems**

Mohammed Al Mahdi and Daniel Kearl

University of Louisville – College of Business

CIS 481: Intro to Information Security

Prof. Steve Kendra

April 4, 2020

Table of Contents

[Table of Contents 2](#_Toc36913547)

[Executive Summary 4](#_Toc36913548)

[Overview 4](#_Toc36913549)

[The Problem 4](#_Toc36913550)

[The Solutions 4](#_Toc36913551)

[Basics of Network Vulnerability 5](#_Toc36913552)

[Benefits of an IDPS 5](#_Toc36913553)

[Threats to Network Security 6](#_Toc36913554)

[Network Attacks 6](#_Toc36913555)

[Phishing 7](#_Toc36913556)

[Ransomware 7](#_Toc36913557)

[Man-in-the-middle 8](#_Toc36913558)

[Packet Sniffing. 8](#_Toc36913559)

[Wireshark and Network Miner. 9](#_Toc36913560)

[DNS Spoofing 9](#_Toc36913561)

[Denial of Service 9](#_Toc36913562)

[Exploitation 10](#_Toc36913563)

[Misconfiguration 10](#_Toc36913564)

[Social Engineering 11](#_Toc36913565)

[Detection and Prevention 11](#_Toc36913566)

[Physical Security 11](#_Toc36913567)

[Access Control 12](#_Toc36913568)

[Business Policy 12](#_Toc36913569)

[Employee Training 13](#_Toc36913570)

[Software Solutions 13](#_Toc36913571)

[Honeypots 13](#_Toc36913572)

[Firewalls 14](#_Toc36913573)

[Redundancy 14](#_Toc36913574)

[Load Balancing. 15](#_Toc36913575)

[Parallelism. 15](#_Toc36913576)

[Network Isolation 16](#_Toc36913577)

[Proxies. 16](#_Toc36913578)

[Virtual LANs. 17](#_Toc36913579)

[Encryption 17](#_Toc36913580)

[Network. 18](#_Toc36913581)

[Mechanics. 18](#_Toc36913582)

[Data. 19](#_Toc36913583)

[Maintenance 19](#_Toc36913584)

[Scheduled Downtime 20](#_Toc36913585)

[Update Management 20](#_Toc36913586)

[Recovery 21](#_Toc36913587)

[Management 21](#_Toc36913588)

[Contingency Planning 22](#_Toc36913589)

[Incident Response Plans. 22](#_Toc36913590)

[Disaster Recovery Plans. 23](#_Toc36913591)

[Business Continuity Plan. 23](#_Toc36913592)

[Evaluation 23](#_Toc36913593)

[Conclusion 24](#_Toc36913594)

[References 25](#_Toc36913595)

Executive Summary

Overview

Organizational network security is an increasingly more important topic for both businesses, employees, and even individual users, as technology throughout the world evolves at a pace that was once unimaginable.

The Problem

Organizations, especially smaller businesses, are often much more vulnerable to network attacks than they typically assume. This is already an issue on its own, but with many more businesses moving to online operations for the first time, it’s important that security practices are familiar to those who need them the most.

As mentioned previously, it’s not just businesses who need this information, the target for a lot of these vulnerabilities end up being employees or everyday users, who often would be much more secure if even just simple knowledge of potential vulnerabilities had been presented to them before a real attack occurs.

The Solutions

There is no one solution to this issue. Not only should more people be informed, but there are measures to be taken beyond simply providing information that can greatly improve the security, safety, and privacy of organizations and their members.

The goal of this paper is to present these many solutions to the problems that organizations face, with the goal of moving those who were potentially unaware of some of the issues toward a more secure solution.

Basics of Network Vulnerability

Network Systems attacks are increasing every day, and many organizations suffer from these attacks as they are the main targets for them. There are many reasons why attacks are mainly focused on organizations, one of the reasons being competitive intelligence: the attacker wants to know secrets about the organization’s financials, products, services or other business secrets. Another main reason for targeting organizations is the potential to disrupt critical operations, via Denial of Service or ransomware attack, among others. In these attacks, the attacker intends to harm or disable the organization’s network operations, for any wide array of reasons they may have. In order to prevent these attacks from affecting your organization it is recommended that you have an Intrusion Detection and Prevention System (IDPS) in place, because a good IDPS will closely monitor and analyze computer network traffic, opening up the potential for detecting any intrusions or other anomalies, and then notify a systems administrator in an event of an attack or suspicious activity on the network.

Benefits of an IDPS

Network Intrusion Detection and Prevention Systems (N-IDPS) can be deployed using a hardware or software sensor or agent, which are commonly installed on the network gateways with other networks (like the internet) as those areas are ideal for scanning the most incoming and outgoing traffic from the network, or north-south traffic. The central machine is a system that stores data in a location in which it can be used for logging, alerting and reporting when a sensor detects an unusual activity. Typically, the more effective of these systems run via anomalous detection, which means they “study” network activity, and when something differs greatly from typical traffic, it raises red flags for further investigation by administrators.

A Host IDPS (H-IDPS) works differently to accomplish the same goal. An IDPS can only control or scan what it has access to, or what it can “see.” This means that an N-IDPS may be very good at detecting odd traffic in and out of an organization’s network, but it’s not going to see very much of the inside traffic between hosts, or east-west traffic. For that, an H-IDPS is implemented. This is most commonly software that is found on individual hosts on the network, that all perhaps report back to one central IDPS server, where all data can be congregated and analyzed by a security professional at the organization. These two technologies work together to provide thorough coverage of an organization’s network activities, effectively highlighting anything out of the ordinary that may occur throughout its systems.

Threats to Network Security

Network Security refers to the ability to protect the network as the name implies, meaning network security threats are potential risks that can or will negatively impact any organizational network assets. As mentioned previously, threats to network security are increasing in frequency and severity on a daily basis, affecting many business organizations in entirely different ways. In order to prevent more of these attacks from having such an impact, it is crucial that the proper systems are in place to detect and subsequently prevent any serious threat as soon and as thoroughly as possible. The types of attacks and techniques for intrusion vary in breadth, purpose, and application, and here you will see a little bit of everything in terms of what to expect attackers to use against an organization.

Network Attacks

Some of the more malicious threats one would see facing an organization include several basic network-originating attacks. In theory, these attacks are always a potential threat to an organization from the beginning, in the sense that one could happen at any time, though the likeliness of one can very greatly. For example, a small business without much of an online presence could theoretically be subject to a DoS or DDoS attack at the office, but it wouldn’t be very effective or productive for the attacker, and as a result is relatively unlikely. Malicious attacks like phishing or ransomware are much more likely to be a concern for this organization, because even without much online presence, that business undoubtedly has data somewhere on their network. This data would be valuable to an attacker to obtain control of, whether that’s via a ransomware attack to get money out of the business, or a phishing attack to get access to sensitive files.

Phishing

According to the Principles of Information Security book, the definition of Phishing is an “attempt to gain personal/confidential information; apparent legitimate communication hides embedded code that redirects users to a third-party site.” This means that the attacker will trick an employee into entering personal information, credentials, or other details into a form that may look very much like a real, legitimate site, even one as familiar as an organization’s internal employee portal. After they get these details, they could use them to lock employee accounts, retrieve sensitive or confidential data, install malicious software, or otherwise disrupt business operations, all because one employee gave up access credentials while filling out a phishing form that looked completely normal to them. In order to prevent phishing from happening to your organization, proper employee training is required and must be done often (perhaps quarterly) in order to keep the team informed. This can’t be all though, another very effective method of preventing things like the above from happening is proper access control. Limiting access to assets from one login can limit the amount of damage an intruder can do to an organization that is compromised by a phishing attack.

Ransomware

Ransomware is a common type of malware that will encrypt any files within its reach, making them inaccessible to the intended user. These infections then will display a screen asking for money in return for a key that can decrypt the affected files. What’s especially dangerous about this malware is that if the computer infected is on a network, and depending on the complexity of the malware, it could infect other computers connected to the same network. This has the potential to cause plenty of expensive damage to an organization. In 2017, a ransomware cyber-attack known as “WannaCry” hit hundreds of United Kingdom National Health Service (NHS) computers. As a result, many hospitals were forced to delay surgery and cancel patients’ appointments, causing harm not only to several organizations but to individuals as well. The impact of WannaCry doesn’t stop there, many other organizations have been hit, including some as large as FedEx or Nissan. To effectively protect your organization from WannaCry or any future Ransomware, always have active back-ups to mitigate the effect of a successful attack, and deploy effective anti-malware or H-IDPS software for clients and servers, to lower the odds and/or limit the spread of successful infections. User training is also very effective in this attack, as is the case for almost any intrusions that depend on users as a weak point.

Man-in-the-middle

According to the Principles of Information Security book, “in a man-in-the-middle attack (MITM) or TCP hijacking attack, an attacker sniffs packets from the network, modifies them, and inserts them back into the network.” This essentially means that an intruder could see what a client intends to send to a server, intercept that communication, and then send something different instead. One of the most common man-in-the-middle attacks requires an attacker to set up a mobile Wi-Fi network in a public place like a coffee shop, restaurant, or shopping mall. People then connect to the wireless network assuming it’s the public network provided by the place they’re visiting, and once they connect, the attacker is then able to steal any logins, passwords, even data like credit card numbers passed over this Wi-Fi by an unsecured host. To prevent these attacks, according to the National Institute of Standards and Technology (NIST) there are Wireless IDPS sensors that can detect when an attacker is trying to spoof a Wi-Fi network, which can identify the physical location of the detected threat using triangulation. Wireless IDPS sensors can be placed in multiple locations in the organization building and even in public, to protect users from any MITM attacks. In addition, an individual user can protect themselves by refraining from using public networks altogether, though if unavoidable, using an encrypted VPN tunnel to transfer data will prevent eavesdropping.

Packet Sniffing.

Packet/network sniffing, also known as packet analyzing, employs pieces of hardware and/or software that monitors traveling data over a network. Most organizations use these for legitimate purposes like keeping track of employees’ network use or adding additional protection from malicious communications (Critelli, 2019), although they can be used maliciously by an attacker to steal information traveling over an unsecured network in a similar fashion.

Wireshark and Network Miner.

Wireshark and Network Miner are similar programs that can be used to analyze packets on your network which then capture network data traveling through the network. Both Wireshark and Network Miner can be helpful to see what is going on over a network, as these tools are commonly used by network administrators to troubleshoot network problems or to examine security vulnerabilities. It’s always important for a network administrator to have a secured and encrypted network to prevent any unauthorized user from capturing or analyzing organizational data as this tool can also be used against your organization.

DNS Spoofing

Domain Name System (DNS) Spoofing is an attack in which a cyber attacker alters a DNS cache in order to trick a victim’s computer into going to an illegitimate address using a perfectly legitimate domain name. Proper network monitoring should largely prevent these kinds of attacks because for this attack to be performed, the victim’s computer typically must make a DNS request to an attacker’s server to obtain the malicious address masked by the legitimate domain name. Blocking DNS requests going to anywhere other than pre-approved DNS servers (whether that’s an internal DNS server or one commonly used, like Google or Cloudflare DNS) should prevent the victim from obtaining the malicious address altogether.

Denial of Service

During a Denial of Service (DoS) attack the attacker sends a massive number of packet requests to a server, during which the server becomes overloaded with packets and cannot respond to any incoming requests. This causes massive slowdowns and potentially crashes of the receiving server, rendering it unable to perform any normal functions. A Distributed Denial of Service (DDoS) attack is like a DoS attack but instead of originating from one host, the attack comes from many different areas, usually from bot computers which are controlled by the attacker(s). A DDoS attack is usually harder to combat as it comes from multiple locations while a DoS attack usually comes from one IP address which could simply be blocked. For an organization to stay protected from DoS/DDoS attacks, there are plenty of tools available, from scalable third-party cloud solutions to in-house deployable IDPS or firewall-based solutions. It’s important to pick the proper tool for the job so to speak, because as a business grows, the target on their back will likely grow as well.

Exploitation

Exploitation of a system is different than, but very similar to a typical attack. Exploitation depends on taking advantage of weak points in a system, typically caused by some unintended opening in software or security. These can often be easily fixed, but it’s important to remember that they exist because they were never noticed, meaning they can be exploited at any time without any previous knowledge or preparation for such an exploit to occur. Exploits are often the reason behind software hotfixes, because users may find an opening in software resulting from a patch, and a hotfix is sent out soon after to patch that hole before attackers take advantage of it.

Misconfiguration

Attackers are as clever as they need to be, meaning they can find ways to get into a system via points that are commonly left unconfigured, or are misconfigured when deployed. System misconfiguration is a large threat to organizations because these things are exploits that aren’t caught by the people configuring the system to begin with, meaning there’s no heads-up that an attacker could exploit a misconfigured part of a system. There are many varieties of system configuration, like giving access to users that do not need it, leaving the password to a software suite set to default, or leaving storage containing credentials insecure. It is always important to have proper system configuration to prevent any unauthorized access to a system, always have a system up to date, do not use default credentials, and set proper user access to prevent misconfiguration exploits.

Social Engineering

Social Engineering is exploiting human psychology to trick people using various techniques in order to gain access to system, data, building, or otherwise. Employees need to be trained and prepared for such a threat, especially in outward-facing positions within an organization where one would be more vulnerable to social engineering. The most used technique by social engineers is someone who poses as an IT staff and asks employees for their password in order to fix an issue with their account, but a prepared and vigilant employee would recognize that IT staff should never ask for an employee password for a variety of reasons.

Detection and Prevention

Intrusion detection and prevention systems (IDPS) are hardware and/or software suites that are implemented on a network to act as security features that monitor network activities. These systems detect packets that may possess threats on your organization’s network, either via signature-based detection of malicious software, or (more effectively) anomalous activity detection of activity that is out of the ordinary. In a presentation given by Kaleb Brown on IDPS, it was emphasized that both detection and prevention are critical in protecting a system, but all too often the focus is given to protection. He mentions that it is important to always operate in an “assume breach” manner, meaning it should always be assumed that a system is compromised, and a system should be constantly monitoring activity to detect intrusions.

That’s not all there is to this though. While an IDPS is a spectacular solution to many security-related issues, it’s not a catch-all solution. There are still issues to resolve such as unintended physical access, organizational issues with security typically in the form of policies, all the way down to individual employee behavior that can help or hurt an organization’s security.

Physical Security

Physical security varies a little bit from the typical theme of this topic, because it has to do with physical access to organizational assets. While it may feel like a different subject entirely, it is actually very closely related to the subject of network security, in that if physical security is compromised to critical assets, it may not even matter how secure the network is because someone literally has physical control of what they’re looking for.

Access Control

Access Control is both a method of digital security, and one of physical security. Here we’ll focus more on the physical security side of things since the digital side is better covered elsewhere. Access control ensures that users have appropriate access that is designed to their job title, and while that is true for both digital and physical security, the means of controlling this access is different in each domain. A good example to use as an asset here is a server room. Any access to a server room should be thoroughly documented, and only a few individually selected people should have independent access to it at any time. During a tour of the University of Louisville’s dark room, it was mentioned that access to the room was tightened significantly, and only a small number of people have their own access codes. People who do not need regular access to the dark room do not have a code and must get explicit permission and supervision to access it at any point in time.

Business Policy

An organization must have policy for a large range of different things, from electronic devices and network use to standard guidelines and procedures. A large part of these policies is offloading liability onto employees in the event of potential misuse of business resources. Employees must accept these policies to work at any business, and part of accepting these is accepting the consequences for not following them adequately. Security Guidelines for user access, password requirements, confidentiality and the usage of data are all examples of policies that are put in place by management in partnership with the appropriate authority on the subject (like a team of professionals from the IT department, for example).

Employee Training

Employees are one of the greatest threats to the organization’s security, simply because there can be so many of them, and their experience and preparedness can vary wildly. Employees do make mistakes which could lead to deleting, duplicating or accidentally modifying files, which can all be fixed with simple backups in place, but employees also need to understand the threats they pose to a network. This is critical in preventing phishing, ransomware, and social engineering, as these are some of the biggest threats employees face at a given organization. Proper training greatly reduced the chance of an employee falling victim to these threats.

Software Solutions

The world of network security is complex, too complex for a sensible amount of people to do themselves without some assistance from some potentially equally as complicated (or even some quite simple) technological solutions. There is a wide span of software solutions available to those who wish to tighten up their hold on their network, playing many different roles including vulnerability prevention (or redirection), reaction to threats, or active monitoring.

Honeypots

Honeypots are a very common method of reducing threats to a system by diverting potential attackers’ attention away from critical processes. These honeypots work off a simple concept of luring attackers away from anything critical, simply by acting as a more vulnerable system. Therefore, they’re commonly known as decoys, lures, or even flytraps; they’re meant to trap attackers in a dummy system where no damage can be caused. This makes it easier to prevent any attacks that would originate from these attackers simply because knowing how an attack works on a dummy system would help administrators prepare for a similar attack in a live environment. This is a common method of security in email systems; honeypots are established to attract malicious email so sources of them can be more easily identified and blocked from the rest of the user base.

Firewalls

Firewalls are probably the most common type of network security software in the world. Not only can they be very effective, they’re also scalable, highly configurable, and flexible to different applications. Every consumer-friendly desktop operating system in the world (namely Windows, MacOS, some Linux distributions like Ubuntu) come packaged with their own built-in firewall, in addition to network gateways provided by internet service providers. On top of that, most established businesses will run a dedicated, specially configured hardware firewall on its own dedicated machine for strict but clear control over packets flowing in and out of a network.

Standard firewalls operate essentially by filtering both inbound and outbound packet traffic through a network, either allowing or disallowing packets based on their context. That includes their origin, destination, packet type, etc. The configurability of firewalls makes it easy to do anything from simply allowing all connections to a port on one network host, to specifically only allowing packets of an exact type that are coming from one single origin network. While it’s nice to have that amount of control, it’s likely obvious how much of a headache that may be to configure for a network running a very intricate firewall.

Redundancy

Moving away from the direct attack prevention methods, it’s important to discuss the concept of redundancy in a system. Redundant systems can serve a wide range of purposes very well and are typically implemented to improve uptime or accessibility of a system. Even beyond systems, in some environments it’s not a bad idea to have redundant software configurations, just in case one goes down, like in the event of a hardware failure. Think of it this way: when you buy a car, you typically get two sets of keys. Not because you need two sets of keys to start your car, but because if one of those keys goes missing or the remote stops working, you have another set somewhere that can keep you going. That’s redundancy.

Load Balancing.

Redundancy is a broad concept, so recognizing the different ways it can substantially improve the stability of a system is important. One common use of redundancy is load balancing, or splitting traffic to a specific asset or resource between multiple different handlers. These handlers could be switches, web servers, even datacenters. This implementation of redundancy is in effect in more places than may meet the eye- and that’s the idea. One large perk of load balancing systems is that this allows for maintenance to occur on one server while others pick up the extra load, preventing any perceivable downtime despite having one server offline for a maintenance period. The end goal with load balancing is the average person using their preferred search engine or downloading their favorite video game isn’t going to be slowed down if many other people are doing the same thing, or a server goes offline. The traffic to that asset is balanced across multiple receiving servers to provide a smoother experience and overall higher uptime.

Parallelism.

Parallelism is a similar concept, as it is still a type of redundancy, but it may not be as familiar to people as the other forms. This is the use of two (or more) parallel systems to accomplish a task. Two systems being parallel to each other means that at any point in time, the two systems are effectively identical in what they can do or have access to. Data is constantly mirrored between them in real-time, providing a resistance to failure in a live environment. If something goes wrong in the first system, the second system is working in real-time to accomplish that same task, resulting in zero perceived downtime despite the absence of one system. Anyone familiar with the data storage method of RAID, or Redundant Arrays of Independent Disks, may recognize this type of redundancy as similar to a RAID 1 storage setup, where two or more disks have the exact same data mirrored between them in real time. That’s because a RAID 1 storage array applies this very type of redundancy to prevent data loss. Simple, but effective.

Network Isolation

Following the theme of multiple systems, network isolation is another important factor in network security. Access control on its own would be a whole different topic but will be mentioned here for completeness: In general, it’s a good idea to delegate access to an asset only to the people that need it. For example, someone in the finance department of a firm will need access to certain financial records, but it’s extremely unlikely that they would need access to information controlled by the IT department. In this instance, access to the IT department records would be restricted, and someone in an unrelated department would not have access. This concept applies to entire networks also, simply because it’s easier for an intruder in a system to wreak havoc if they have unfettered access to everything from one point of entry. This intruder may be the orchestrator of a targeted attack, or it could just be some employee from who lost their job this morning. Either way, it’s smart to separate systems if for no other reason than because it lowers the potential attack surface.

Proxies.

Proxy servers are a common method of network isolation, so common that they are used in most homes even without their users’ knowledge. Most people familiar with technology understand that their home network is connected to the internet but isn’t quite “part” of the internet in a way. Well, it’s true that there is separation between the two networks, and it’s because the typical residential gateway modem provided by an ISP acts as a proxy server. Proxies are a middle-man gateway between two networks, breaking direct contact between them. Traffic coming into a network may come through one port, and is distributed to the destination on the internal network through a different port, increasing security through obfuscation of the internal network’s structure, including addresses or other details (“About Proxy Servers,” 2018). Proxies are used in other ways than simply breaking the direct connection between the internet and a home user’s network. A proxy server can be used to mask a user’s information (in the same way it would for a home network) from the server the user may be connecting to. It’s not uncommon for more privacy-centric users to use proxies when browsing the web, usually to prevent trackers from collecting information about browsing habits and attributing it to the user or their network.

Virtual LANs.

Another less common aspect of network isolation comes into play in environments with more infrastructure, typically in business environments where security takes a more apparent role, rather than the average home user’s network. As such, these implementations can get very complex very quickly, but the concept is generally somewhat simple. VLANs, or Virtual Local Area Networks, are features of higher end routers that allow for the separation of devices on a network into what are basically different networks, but only virtually. Setting up VLANs in a router allows for different groups of devices to be isolated from each other without disrupting access to resources on a network or access to the internet. For example, an organization with several departments may have a different office for each department, and each office may then have its own VLAN. This can not only improve security via network isolation, which would be helpful in the case of an intrusion, but may even make it easier for people within one office to share resources over their network, due to having fewer devices resulting in lower perceived complexity to the end user.

Encryption

Here is another “brand” of solution to network security threats: encryption. Encryption itself is not necessarily a software-based solution, but its implementation is commonly seen among software used today. The practice of cryptography, or obfuscation of a message via a little-known code, has actually been around a long time. In fact, the use of cryptography dates all the way back to ancient Egypt, where encrypted messages were once inscribed on a nobleman’s tomb (Sidhpurwala, 2019). Despite being such an old method of security, encryption is still in use today, and not only that, but it is perhaps one of the most important and impactful methods of security to date.

Network.

Encryption is the reason people can feel safe entering any kind of sensitive information on the internet, whether they’re doing their taxes, logging in to their bank account, even just shopping online. If someone’s connection is encrypted, it’s generally safe to assume that the only accessor of information they send at that moment will be the intended recipient. This concept is known as network traffic encryption, which works together with SSL, or Secure Socket Layer, certificates to provide secure access to websites. DigiCert, a widely used and trusted Certificate Authority (CA), outlines the concept of SSL certificates as containers of key pairs that verify the identity of a website and use that information to establish an encrypted connection to the site (DigiCert, 2018).

Mechanics.

While it’s cool that encryption is such a powerful tool in security, it would be nice to know how it works, right? Well, that’s a question with many answers that can get extremely complex. Cryptography is a broad field, with many different methods that achieve different results. But to keep this topic consumable, it can be simplified. Essentially, cryptography works by taking a readable message and manipulating it in some way using what is known as a “key.” This key is kept secret, and only given to those who should be able to read the message. Once manipulated, the message is only readable by parties with the necessary key, and as such can be sent over potentially insecure networks (i.e. the internet), without immediate risk of a third-party eavesdropping on the content of the message. This is a very simple explanation, but the concept itself isn’t nearly as complicated as some of the applications or methods of encryption that have been developed today. An important thing to note about the concept of encryption is that it is like, but not the same as encoding. When simply encoding a message, the method used to encode it is generally not kept private, as encoding does not serve a security purpose as much as it does a data integrity purpose. While encrypting a message does encode it by definition, encryption relies strongly on keeping that key as secure as possible to protect the data, like one would protect the key to their home.

Data.

The use and value of encryption doesn’t stop with transmitting messages over insecure networks, not by a long shot. Encryption is often also used when storing sensitive data, using the same general method. This is often referred to encryption at rest. For example, a clinic may keep medical records of their regular patients, and while according to the Office for Civil Rights, encryption at rest is not mandatory for medical records covered by HIPAA (Office for Civil Rights [OCR], 2013), they believe it is their duty to keep patient data as secure as possible. To do this, they encrypt all hard drives containing patient data with a key stored on a different physical drive. This is done to retain the confidentiality of the data if physical control over the drive in-question is compromised.

Encryption at rest isn’t just some enterprise data confidentiality solution though. Most popular desktop operating systems are equipped with file systems that support encryption out of the box. MacOS and Windows 10 Pro users, for example, have the option to seamlessly encrypt their drives using technology built into the operating system. While that’s very nice for the more security-conscious out there, it is important to remember that with an increase in security, there comes a potential decrease in availability (or at least convenience). If that encrypted drive needs to be moved to another computer, it must first be decrypted for its data to be recoverable. The effectiveness of encryption can have more severe downsides, as outlined in the earlier portion covering ransomware attacks.

Maintenance

Just like any physical machine, virtual machines need maintenance too. A factory full of manufacturing equipment would be nothing without regular maintenance and occasional inspection (as has surely been evidenced in the past), and that rule translates well to the world of computer systems. While that’s no secret, it may be a bit more involved when an organization decides it’s time for that long-neglected maintenance session. Especially in larger organizations, where the necessary uptime hours border on 24/7, maintenance is crucial in the proper operation of a computer system. In any instance, the worst downtime is unplanned downtime, and a great way to accumulate some unplanned downtime is to skip regular maintenance.

Scheduled Downtime

Computer’s don’t have to sleep, but people do. Unfortunately, systems administrators don’t really get to sleep when other people do, because they’re probably the ones keeping systems in their respective organization afloat. A major key to keeping things running smoothly during working hours in a business environment is proper maintenance planning. Maintenance can mean downtime, so when it inevitably needs to happen, it’s better to have a schedule for it. Most people work during daytime hours through the week, with time off on the weekends and at night, so what better time to bring the servers down than at night on a weekend? It is common practice (and rightly so) to perform maintenance that requires downtime on critical systems when the least amount of people will be impacted. Whether that’s at night on the weekend or bright and early Wednesday morning is a decision left completely up to individual organizations’ management and IT department.

Update Management

Another common practice in the world of systems administration is update management. Software updates are important, both in business and environments and for home users, because as software gets outdated, more vulnerabilities are found. Leaving major software out-of-date, especially something like an operating system, broadens the potential attack surface of a system, opening the host computer and its entire network to unnecessary vulnerabilities. To prevent this, running regular updates on major software (anti-virus, anti-malware, anti-spyware) and the operating system make up most of the protections recommended by the FBI’s cybercrime division (FBI, 2016).

Initially starting with Microsoft, many software vendors have come to release patches for their products on Tuesdays, and fixes for exploits on Wednesday if necessary. This is unofficially known as Patch Tuesday, due to the practice becoming so common among different vendors and organizations. While Tuesday is probably a great day for software developers, giving them the rest of the week to iron out any bumps that crop up from Tuesday’s release, it can sometimes be a bit inconvenient for businesses to run updates on Tuesday when employees are busy. That’s where update management comes in with its multi-phase approach to making software updates more manageable.

Recovery

In any environment, be it a large organization or simply a home user, recovery from intrusions is a critical step in getting things back to normal. In fact, it’s essentially required. And as such, it should be done properly to ensure that anything affected by an intrusion is safely restored as close as possible to its state prior to tampering. In addition, application of additional security measures may be necessary to help ensure that a similar intrusion is unlikely to happen again in the future. A solid recovery can also act as its own type of prevention, because the steps taken here toward a more secure environment will absolutely help prevent any future attacks or intrusions.

Management

As with most things in an organizational environment, it all starts with management. Anything relatively major or that may cost more than a couple dollars is probably going to need management’s approval, and specifically with recovery operations, management’s initiation. See, recovery of a large, potentially business-critical system isn’t something that can be left entirely on the shoulders of IT. Recovering from an attack or intrusion, whether major or minor, is a matter that can affect the stability of an organization, and should have attention from the decision-makers at the top of the list. Managers should take a large interest in ensuring that while they may not be the ones out there doing the hands-on work to recover physical systems, they should be able to provide appropriate resources to those who are. Management cooperation and even involvement are critical in the success of a system recovery operation.

Contingency Planning

As mentioned, managers are probably not going to be the ones out there in the field working on the system itself. That job is better left to IT and security professionals to ensure the right steps are taken technologically. That’s not to say that management is only around to write checks and sign off on paperwork, though. Management in an organization plays a critical role in this portion of network security: planning and decision making. While the topic of recovery tends to face the past, asking questions like “what happened” or “how do we prevent that from happening again,” it’s equally as forward-thinking as well. The managerial aspect of recovery is almost entirely future-based, because having an established plan for what to do in the case of an intrusion is critically important, and can cut down on much confusion, frustration, and even work to be done, in the instance when something does actually go wrong. Typically, there are three major types of managerial plans that pertain to information security. These three plans vary in their depth and detail, but they all hold the common focus of minimizing as much damage as possible and keeping the business afloat.

Incident Response Plans.

The most specific type of plan is an organization’s response (IR) plans. These plans are intended to provide a routine that can be followed in the event of a certain type of incident, that will keep business operations up and running as efficiently as possible. There are often many of these, each having its own incident to focus on. These plans can be very specific, but there should be several of them to cover many areas. Incident response plans are the lowest-level plan in terms of severity and are to be executed whenever anything happens that has a plan associated with it. Power goes out in a datacenter? DDoS attack? Follow the incident response plan associated with those issues. In any situation, the incident response plan should be thorough enough to cover the issue at hand, but they must also be tested for this to be the case. On a rainy day, it’s a good idea to simulate incidents that these response plans will cover, to ensure that the steps they outline are effective at solving any problems. If the incident becomes more severe however, then the simple incident response may escalate to disaster recovery.

Disaster Recovery Plans.

Disaster recovery (DR) plans are a little more involved. These are to be implemented whenever an organization encounters a proper disaster that has a greater effect on operations than a simple incident, like a DDoS attack. There’s no hard line that defines what a disaster can or can’t be considered, that decision is left up to the managerial contingency planning team to determine what kinds of events warrant a disaster recovery plan as opposed to simply an incident response plan. Usually a disaster is something that would fully disrupt critical operations in a business for an unreasonable amount of time. How long that time is, and what a critical operation may be, are two of the big decisions left up to the management team to determine. However, these plans do all generally follow a similar primary objective of restoring systems at the original site after disasters occur (Whitman & Mattord, 2018).

Business Continuity Plan.

A business continuity (BC) plan is a little bit different than the other two previously mentioned. The main goal of one is to ensure that the business stays operational, even if that means re-establishing critical systems elsewhere. Typically, the BC plan will run alongside the DR plan if the damage to the organization is large enough to warrant it. This plan is generally very broad and covers only large-scale events, but they are still developed by the same team that will develop IR and DR plans, so it’s important to know that all plans in an organization are made with some form of synergy in mind.

Evaluation

Another large portion of recovery that can tremendously increase effectiveness of any actions taken toward preventing further issues in the future is evaluation. This step is crucial to determine what went wrong, where the intrusions came from, when they began, access that resulted from said intrusion, or any detail about what may have happened related to an intrusion. These details can be used in standard recovery processes, perhaps outlined in an incident response plan, to reinforce areas that may have been weak, as can be observed in this evaluation phase. Just knowing what went wrong is half the battle, because once systems administrators have that information in front of them, it just comes down to finding good ways to patch up the security holes that may have been exploited.

Conclusion

To conclude, it’s important to note that network security in organizations is becoming ever more important, especially as the evolution of technology continues and more businesses are making the switch to internet-based operation. Keeping a business secure previously only had to do with the lock on the front door, and for many businesses today, their security is now all about keeping their network infrastructure secure in any way they can. Many network administrators deploy Intrusion Detection and Prevention Systems (IDPS) to solve much of this problem. Due to the ability of these IDPS to quickly and accurately identify potential threats to a network, organizations around the world are just a little bit safer.

References

Bugcrowd. (2017, June 15). What is responsible disclosure? https://www.bugcrowd.com/resource/what-is-responsible-disclosure

Critelli, A. (2019, November 19). Packet sniffer basics for network troubleshooting. Red Hat. https://www.redhat.com/sysadmin/packet-sniffer-basics

DigiCert. (2017, May 23). *What is SSL (Secure Sockets Layer)?* <https://www.digicert.com/ssl/>

Federal Bureau of Investigation. (2016, May 3). Cyber crime. https://www.fbi.gov/investigate/cyber

Indiana University. (2018, November 15). *About proxy servers*. Indiana University Knowledge Base. <https://kb.iu.edu/d/ahoo>

National Institute of Standards and Technology. (n.d.). Intrusion detection and prevention systems. TSAPPS at NIST. https://tsapps.nist.gov/publication/get\_pdf.cfm?pub\_id=901146

Office for Civil Rights. (2015, December 18). *Is the use of encryption mandatory in the security rule?* HHS.gov. <https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html>

Sidhpurwala, H. (2013, August 14). *A brief history of cryptography*. Red Hat Security Blog. <https://access.redhat.com/blogs/766093/posts/1976023>

Whitman, M. E., & Mattord, H. J. (2018). Planning for security. In *Principles of Information Security* (6th ed., p. 216). Cengage Learning.