OSIbeyond

6 Critical Cybersecurity Policies Every Organization Must Have

August, 2020

Contents

6 Critical Cybersecurity Policies Every Organization Must Have

Introduction

All modern organizations—regardless of their size, location, and domain—are confronted with cybersecurity threats ranging from minor to critical. Such threats include phishing attacks, ransomware and other malware, insider attacks, Denial-of-Service (DoS) attacks, and others.

While some organizations take these threats seriously and know how to protect themselves against them, cybercrime statistics show that most are alarmingly unprepared, leaving them vulnerable to cyber-attacks that could potentially threaten their very existence.

According to Bitdefender's Hacked Off! report, 57 percent of companies have experienced a breach in the past three years, and nearly the same number (60 percent) was published by the enterprise technology market researcher Vanson Bourne and the insurance firm Hiscox (61 percent).

In 2020, the average cost of a data breach is expected to exceed $3.8 million, according to the 2020 Cost of a Data Breach Report published by IBM Security, and large enterprises will not be alone in paying the price for insufficient cyber readiness. That's because 43 percent of the cyber-attacks launched today target small and medium size organizations.

Cybercriminals are increasingly targeting small and medium size organizations because they know that such organizations are far less likely to have well-designed cybersecurity policies than large enterprises with dedicated security teams and deep pockets.

Without cybersecurity policies outlining how to keep threats at bay and clearly stating what needs to be done when they do occur, small and medium size organizations are at a huge disadvantage in today's world, where costly breaches and cyber-attacks are the new normal.

However, that's not how things have to be. Regardless of size and budget, all organizations can and should create at least the most critical cybersecurity policies to protect their data and comply with various regulations, such as PCI, HIPAA, GDPR, and others. With documented cybersecurity policies in place, employees will know what to do and what not to do to prevent a network intrusion and reduce its impact.

This eBook describes six critically important cybersecurity policies that no organization can afford to ignore if it wishes to maintain its competitive edge. We explain the purpose of each policy and provide practical tips and advice on how to create and implement them so that small and medium size organizations that have no previous experience with them can avoid making costly mistakes in the early stages.

1

Acceptable Use Policy

Policy Overview

The purpose of an acceptable use policy is to describe what employees can and can't do when using the organization's IT equipment or accessing its network over the internet.

This cybersecurity policy addresses the fact that human error is the main cause of 95 percent (or 19 out of 20) of cybersecurity breaches. From clicking on malicious links to accessing sensitive data using personal devices, there are many things most employees do on a daily basis that can open the doors to a cyber-attack.

By formalizing constraints and practices that all employees must agree to and abide by, organizations can effectively strengthen their cybersecurity defenses without spending any money on a costly cybersecurity solution or burdening their IT departments with even more responsibilities.

Since all organizations are different, it's important for each organization to create an acceptable use policy that addresses the issues it's facing and reflects the IT equipment available. Only then can the policy effectively direct responsible behavior.

Why Is This Policy Important?

In a perfect world, employees would always use computing devices only for work-related purposes, and they would never knowingly or unknowingly do anything that could expose the organization to a cyber-attack. Unfortunately, we don't live in a perfect world and end user actions are the most common entry point for threats into a network, according to the SANS Institute 2016 Threat Landscape Survey.

Because more and more employees are blurring the lines between personal and work devices, the risk of end users causing a breach will only keep increasing unless organizations take concrete steps to address this problem.

Employee computer monitoring was an effective means of catching misbehaving employees red-handed in the past, but it's far less effective in the bring your own device (BYOD) era, with employees seamlessly switching between personal and work devices during the day.

The solution is to make employees accountable for their actions by spelling out a specific set of rules they must follow when using the organization's IT equipment or accessing its network over the internet. When employees are held accountable by a well-documented policy with clearly described sanctions, they are much more likely to think twice about their IT-related worktime activities.

What Does an Acceptable Use Policy Include?

Most acceptable use policies are only a few pages long, clearly organized into sections and relying heavily on numbered lists and bullet points to make them as readable as possible. By far the most important section of an acceptable use policy is the one with specific rules that employees are expected to follow.

Here are some examples of such rules gathered from various acceptable use policies:

- Sharing of passwords, PINs, tokens or other authentication information is strictly prohibited. Each individual is responsible for his/her account(s), including the safeguarding of access to the account(s). (Source)
- While traveling on vacation, you ask a staff person to check your email for you by forwarding your email to their account, removing the forwarding on your return. (Source)
- Prohibited use: Browsing explicit pornographic or hate-based web sites, hacker or cracker sites, or other sites that the corporation has determined to be off-limits. (Source)
- Agree to handle all information stored on a computer or downloaded to portable media such as flash drives and hard copies with appropriate care to prevent unauthorized disclosure of the information. (Source)
- Employees may not use the company's Internet connection to download games or other entertainment software, including wallpaper and screen savers, or to play games over the Internet. (Source)

Other important elements of an acceptable use policy include those dealing with the scope of what the policy covers, definitions of important terms, and penalties for non-compliance with the rules.

How to Create and Implement an Acceptable Use Policy?

Writing an acceptable use policy from scratch is not necessary anymore since there are many free templates based upon various industry frameworks, such as NIST, PCI, HIPAA, SOC 2, or ISO 27001. Regardless of if you use a template or do everything by yourself, here are some things to keep in mind when creating and implementing an acceptable use policy:

- **Promote good cybersecurity practices:** Your goal should always be to promote good cybersecurity practices—not arbitrarily enforcing a specific way of working. As such, it's important to identify the most dangerous attack vectors and threats that employees deal with on a regular basis and create rules that directly combat them by addressing a certain behavior.
- **Perform an annual refresh:** Technology advances at a rapid pace and an acceptable use policy can keep up with it only when it's regularly updated to reflect changing working habits and trends. Another advantage of performing an annual refresh is that it reminds employees of its existence and content so that it's not just new hires who follow it.
- **Ensure its legality and enforceability:** For an acceptable use policy to be taken seriously by employees, it needs to have a solid legal footing and be enforceable. The last thing any organization wants is to spend valuable time crafting an acceptable use policy only for employees to discover that it violates their rights and is thus impossible to enforce.
- **Make it clear:** An acceptable use policy should be a cross between a legal document and a guide. It doesn't need to explain the reasoning behind the rules it contains, but it needs to be written clearly enough for employees to easily understand them. Likewise, an acceptable use policy should be written using a language that's broad enough to prevent technical loopholes but, at the same time, detailed enough so that it's clear what the policy is talking about.

2

Security Awareness Training

Policy Overview

Security awareness training aims to provide formal cybersecurity education to employees, equipping them with the knowledge they need to identify and avoid cybersecurity threats. It addresses the fact that employees can't be expected to keep up with the rapidly evolving cyber threat landscape since they have other responsibilities to focus on.

In a way, security awareness training serves as the first line of defense when it comes to securing networks and sensitive data sent across them. The 2014 US State of Cybercrime Survey revealed that organizations with a security awareness training policy in place had an average financial loss of $162,000, while organizations without one reported an average of $683,000.

To deliver the biggest positive impact possible, security awareness training should encompass not just new hires but also existing employees who have been with the organization for some time. An annual refresher in a conference room is a good start, but modern technology makes it possible to significantly increase the effectiveness of security awareness training by introducing gamification elements to make the training more interactive and thus engaging.

Organizations can even offer prizes for employees who score the most points during various security awareness training exercises, such as interactive quizzes covering common cybersecurity threats and the ways to combat them.

Why Is This Policy Important?

Long gone are the days when the IT department had total control over the devices and software used by employees. Today, many organizations actively encourage employees to bring their own devices to the workplace and continue using them for work-related purposes at home. Employees themselves have gotten accustomed to various online services and applications, many of which introduce risks related to data security and privacy.

As such, security has become everyone's responsibility. The problem is that not all organizations have been able to get this message across and teach employees that even seemingly harmless behaviors can lead to major security incidents. According to a report called 2020 Cost of Insider Threats: Global Report, the number of insider-caused cybersecurity incidents increased by 47 percent since 2018, and their average annual cost jumped up by 31 percent, reaching $11.45 million.

Statistics like these highlight the need for more comprehensive security awareness training policies. When implemented correctly, security awareness training has been found to reduce the risk of certain cyber threats, such as social engineering attacks like phishing, by as much as 70 percent.

What Does a Security Awareness Training Policy Include?

A good security awareness training policy establishes the requirements for employees, management, and IT staff to complete security training programs in order to learn how to protect important data and systems against cyber threats.

Here are some examples of such requirements gathered from various security awareness training policies:

- University staff and employees are required to complete an annual online Security Awareness Training course every twelve (12) months. All newly hired employees are required to complete the Security Awareness Training course within the first 30 days from the date of hire or prior to receiving access to the University's IT systems and data. (Source)
- Community Health Plan will run anti-virus software on all computers that connect to the internet and/or are networked together. Members of the workforce must be trained on how to use the software and how to spot unusual activity that might indicate the presence of a virus. The anti-virus software must be kept up to date, as new viruses (and other types of malicious code) are discovered daily. (Source)
- Resolver has developed specific security policies to identify core activities such as security reminders, protection, login monitoring, and password management. All Full time and Contract staff are

trained on these policies as part of their orientation. (Source)

In addition to individual training requirements, a security awareness training policy should cover the responsibilities of different employees and explain the consequences for failing to comply with the policy.

How to Create and Implement a Security Awareness Training Policy?

Each organization has a different IT infrastructure, employee turnover rate, and cyber defense capabilities, and it's important for a security awareness training policy to reflect all these and other factors to be as effective as possible. The creation of a security awareness training policy should be the responsibility of appropriate security or IT staff, and management must both enforce the policy and lead by example.

The National Institute of Standards and Technology (NIST) published a comprehensive guide with templates for building an information technology security awareness and training program. The guide covers everything from designing an awareness and training program to developing educational material for it to its actual implementation, and all organizations that have no previous experience with creating and implementing a policy like this should at least quickly go through it.

The following security awareness training tips and strategies can transform a good policy into an excellent one:

- **Focus on the greatest risks:** Not all cybersecurity risks are equally dangerous. For example, social engineering attacks like phishing are responsible for significantly more data breaches than SQL injection attacks. That's why it makes sense to make the greatest risks the focal point of security awareness training.
- **Mix theory with practice:** The fact is that most employees are not personally interested in cybersecurity and don't find PowerPoint presentations on the topic engaging. Practical cyberattack simulations are a great way how to make training more effective and, at the same time, demonstrate its importance.
- **Monitor compliance:** After implementing a security awareness training policy, it's crucial to put in place compliance monitoring processes. The gathered data can reveal dangerous gaps and suggest appropriate corrective actions.
- **Collect feedback:** A security awareness training policy is valuable only when employees adhere to it, and that's much more likely to happen when they actually agree with it. By collecting feedback from employees, organizations can periodically revise their policies to reflect the opinions of those who are affected by them.

3

Identity Management Policy

Policy Overview

Identity management policy, also referred to simply as identity management, is an IT security discipline that deals with the management of digital identities and the privileges associated with them. It encompasses everything from the provisioning of identities to authentication mechanisms to employee offboarding.

An identity management policy aims to grant the right users access to the right information and systems in the right context. When implemented correctly, it significantly decreases the risk of a data breach caused by the organization's own employees, and, at the same time, relieves IT staff from many of the routine tasks associated with identity management.

In recent years, the General Data Protection Regulation (GDPR) and other sweeping data protection and privacy regulations have highlighted the need for strong identity management policies, forcing even organizations that previously didn't consider identity management to be particularly important to make it their priority. The good news is that organizations of all sizes can choose from a broad range of identity and management technologies to manage access rights more efficiently.

Why Is This Policy Important?

According to IBM's 2016 Cyber Security Intelligence Index, approximately 60 percent of all data breaches are caused by an organization's own employees, with 75 percent of documented incidents being malicious in intent and 25 percent being accidental.

This and other similar statistics serve as proof of what security experts have been saying for years: users are the weakest link in security. To strengthen this weak link, it's essential to ensure that users never have more access privileges than they absolutely need.

Of course, it's relatively easy to remove access to critical systems and sensitive information, but doing it in a way that doesn't impede productivity can be a real challenge. That's why an identity management policy should be an integral part of an organization's security plan and not just an afterthought.

When implemented correctly, an identity management policy can greatly enhance productivity of both regular employees and IT staff.

More and more organizations today encourage employees to work remotely, often using their personal devices. Identity management systems make it possible to give users outside the organization access to internal systems in a safe, controlled manner. It also decreases the number of help desk tickets IT staff has to deal with on a daily basis, making its implementation one of the best decisions any organization can make.

What Does an Identity Management Policy Include?

A well-written identity management policy addresses how identities are authenticated, authorizations managed, and accounts and privileges deprovisioned. Its scope includes both individual account holders and information system operators responsible for identity management systems.

The following requirements can be found in many identity management policies:

- Create passwords that conform to best practices for selecting passwords which address length and complexity. (Source)
- The access rights of all employees, students and associate account users to information and information processing facilities will be removed upon termination of their employment, contract or agreement, or adjusted upon change. (Source)
- Where possible, all default user accounts will be disabled or changed. These accounts include "guest", "temp", "admin", "Administrator", and any other commonly known or used default accounts, as well as related default passwords used by vendors on "commercial off-the-shelf" systems and applications. (Source)

An entire section is typically dedicated to password requirements to ensure that all passwords are adequately strong and unique. Common password requirements include password expiration, minimum length, password complexity, and password history, just to name a few. It's always a good idea to encourage multifactor authentication when reasonable to do so because it greatly reduces the risk of an unauthorized intruder gaining access to an important system.

How to Create and Implement an Identity Management Policy?

When creating an identity management policy, it’s important to cover the following:

- **The authentication process.**
  Example: The requirement to use multifactor authentication, such as a password in combination with biometric authentication.
- **The authorization to use a resource associated with an account.**
  Example: The segmentation of user privileges across separate users and accounts to decrease opportunity for conflict of interest or fraud.
- **The responsibilities of regular employees.**
  Example: Password creation and use requirements.
- **The responsibilities of information systems staff.**
  Example: Close monitoring of failed login attempts and other suspicious activity.
- **The removal of an employee’s authorizations and accounts.**
  Example: The accounts belonging to employees who no longer work for the organization must be deleted.

Because all organizations are different, it’s best to start with an audit to define the organization’s needs, which should also guide the selection of identity management tools. After its implementation, the identity management policy should be regularly reviewed and updated when necessary.

4

Disaster Recovery & Business Continuity

Policy Overview

Disaster recovery and business continuity are two closely linked practices whose purpose is to prepare an organization for disruptive events, helping it resume operation as quickly and painlessly as possible. Disruptive events in the context of disaster recovery and business continuity include everything from brief power outages to cyber-attacks to country-wide national disasters.

Because of their closely linked nature, the terms disaster recovery and business continuity are often used interchangeably even though they are anything but interchangeable. This is how Disaster Recovery Journal defines the two terms:

- **Disaster recovery:** The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organization after a disaster or outage.
- **Business continuity:** The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.

In other words, disaster recovery is a subset of business continuity, dealing with information or technology systems that allow the organization to operate. However, recovering technology alone isn't enough to get the organization back on its feet.

For that to happen, other resources supporting essential functions must be recovered as well, including people, infrastructure, and contracts. The recovery of these and other functions necessary to continue business processes is the domain of business continuity.

When disaster recovery and business continuity work together, they ensure the recoverability of all data, systems, and processes.

Why Is This Policy Important?

It's natural for humans to focus on immediate problems and ignore those that may or may not happen in the future. That's why many organizations don't plan for disasters until they are hit by one. According to Nationwide's Small Business Indicator, a majority (68 percent) of small-business owners don't have a written disaster recovery plan even though about half said it would take them at least three months to recover from a disaster.

The problem is that most organizations don't recover. In fact, the British Chambers of Commerce found that 93 percent of businesses that suffer data loss for more than ten days file for bankruptcy within one year. With cyber criminals targeting small and medium-sized organizations at a growing rate, the importance of having a well-thought-out disaster recovery and business continuity policy is easy to understand.

For organizations in certain industries, such as healthcare and finance, formulating a disaster recovery and business continuity policy is also a regulatory requirement.

What Does a Disaster Recovery & Business Continuity Policy Include?

The content of a disaster recovery and business continuity policy depends largely on the size and focus of the organization implementing it. A small retailer with just 10 employees relies on completely different technology and processes than a large logistics company with branches in multiple countries.

That said, all disaster recovery and business continuity policies must address both IT resources and core business functions. The following information can be found in most disaster recovery and business continuity policies:

- **Business impact analysis**
- **Contact information**
- **Infrastructure review**
- **Prevention mechanisms**
- **Recovery technologies**
- **Recovery testing**
- **Recovery Time Objective (RTO)**
- **Recovery Point Objective (RPO)**

Generally speaking, a disaster recovery and business continuity policy should include everything necessary to reestablish an organization's critical business applications and processes after a disaster, including computing, networking, personnel, procedures, and physical facilities.

A good disaster recovery and business continuity policy is easily readable and full of actionable step-by-step procedures for resilience and recovery.

How to Create and Implement a Disaster Recovery & Business Continuity Policy?

Since various organizations rely on vastly different IT systems and business processes, a good first step when creating a disaster recovery and business continuity policy is to perform a disaster recovery business impact analysis, whose purpose is to determine what needs to be recovered and how quickly.

After the most critical aspects of the business have been identified, it's time to describe how the organization will act in an emergency to recover from it as quickly and completely as possible. Organizations that are creating a disaster recovery and business continuity policy for the first time can adopt an existing template, such as the one available at FEMA.

Creating a disaster recovery and business continuity policy typically involves the following steps:

1. The identification of the scope of the policy.
2. The identification of critical business areas.
3. The identification of important functions.
4. The identification of dependencies between various business areas and functions.
5. The determination of acceptable downtime for each critical function.
6. The creation of a plan to maintain operations.

A disaster recovery and business continuity policy should be rigorously tested to verify that it fulfills its intended purpose. For example, many organizations regularly back up important data according to documented procedures, but they never check if the backups are actually recoverable. When a disaster strikes, they are left unrecoverable backups and/or unacceptable long restore times.

5

Incident Response

Policy Overview

An incident response policy establishes processes and procedures to detect, respond to, and recover from security incidents, such as data breaches, malware infestations, and unauthorized attempts to access internal systems and data, just to give a few examples.

A well-established and thoroughly tested incident response policy can be a powerful shield against all kinds of cyber threats, allowing the organization to respond adequately and in a timely manner. What an incident response policy doesn't protect the organization against are physical disruptors, such as power outages and natural disasters, which are in the domain of disaster recovery and business continuity.

Because all organizations deal with different cyber threats, their incident response policies must be created to reflect their unique needs. That said, all incident response policies should identify an incident response team, specify incident handling and reporting procedures (also known as the incident response plan), and implement a feedback loop that would eliminate—or at least significantly decrease—the possibility of the same security incident occurring again in the future.

Why Is This Policy Important?

As the online presence of organizations across all sectors continues to grow, so does their susceptibility to cyber-attacks. While some SMB leaders have convinced themselves that cybercriminals are interested only in large enterprises, cybercrime statistics paint a completely different picture: 67 percent of all SMBs surveyed by the Ponemon Institute in 2018 had already been attacked.

Clearly, any organization can enter the crosshairs of opportunistic cybercriminals, and many cybersecurity experts would argue that it's only a matter of when and how prepared the organization will be.

According to IBM, organizations with incident response policies spend about $1.2 million less on data breaches than organizations without them. What's alarming, however, is the fact that 51 percent of organizations have only an informal response plan that is often applied inconsistently, as revealed by IBM's 2020 Cyber Resilient Organization Study.

In addition to underestimating their susceptibility to cyber-attacks, such organizations often don't realize that it's never possible to ensure that a network is 100 percent secure. Cybercriminals are tirelessly perfecting their tactics, and even the most security-mindful employee can make an unfortunate mistake and unknowingly open the doors to a data breach.

By implementing an incident response policy, organizations recognize the unavoidable fact that security incidents are something they need to actively prepare for because the alternative can be extremely costly and even put their whole existence at stake.

What Does an Incident Response Policy Include?

The content of an incident response policy should reflect its purpose, which is to establish processes and procedures to detect, respond to, and recover from security incidents.

Here are excerpts from real incident response policies:

- Personnel and contractors using the organization's information systems and services are required to note and report any observed or suspected Security Weakness in systems or services. (Source)
- The Computer Security Incident Response Team (CSIRT) detects and investigates security events to determine whether an incident has occurred, and the extent, cause, and damage of incidents. (Source)
- Knowledge gained from analyzing and resolving Security Incidents should be used to reduce the likelihood or impact of future incidents. (Source)

It's a good idea to first identify an incident response team and define the roles and responsibilities of its members. When everyone has a clearly defined role and responsibilities to take care of in case of an incident, the response can be carried out in a timely, effective, and orderly manner.

Next, it's time to create an incident response plan to avoid making last-minute decisions right on the spot. The SANS Institute identifies six key phases of an incident that need to be addressed by an incident response plan:

1. **Preparation:** Preparing employees to handle security incidents.
2. **Identification:** Deciding whether the event really qualifies as a security incident.
3. **Containment:** Minimizing the damage caused by the security incident.
4. **Eradication:** Eliminating the cause of the security incident.
5. **Recovery:** Restoring affected systems and resuming normal operation.
6. **Lessons learned:** Documenting the incident and analyzing its cause.

An incident response policy should also include a comprehensive overview of the current network infrastructure and security mechanisms, a call list, a description of the breach notification process, and a description of any revisions made to the policy.

How to Create and Implement an Incident Response Policy?

An effective incident response policy addresses all six key phases of an incident, identifies an incident response team, and includes detailed information about the network, just to reiterate some of its foundational elements. To create and implement such policy effectively, the organizations should keep in mind the following:

- **Flexibility:** Cybercriminals quickly evolve their tactics in response to the latest trends in cybersecurity, and organizations must evolve their incident response policies to encompass both known threats as well as emerging cyber-attacks. To simplify future revisions, it's useful to make the definitions in the incident response policy broad enough to include all security challenges—existing and new.
- **Cooperation:** A proper response to a security incident in organizations with more than just a few employees typically requires close cooperation of people across departments, and incident response policies should reflect this by engaging different departments both during the planning process and when implementing the policy.
- **Testing:** It's never ideal to learn about the weaknesses of an incident response policy and its implementation only after experiencing a real security incident. Instead, organizations should test their policies beforehand by simulating common types of security incidents and evaluating their ability to respond to them.

6

Patch & Maintenance

Policy Overview

A patch and maintenance policy specifies who is responsible for the discovery, installation, and testing of software patches and describes the conditions under which they are applied.

The need for a well-thought-out patch and maintenance policy reflects the growing number of devices and software applications used by employees working for organizations of all sizes. An unpatched vulnerability may allow cybercriminals to circumvent otherwise robust cybersecurity defenses and steal sensitive information or cause some other disruption.

In the past, patches were relatively easy to apply because most organizations were much less dependent on their IT infrastructures than they are today. Additionally, it took cybercriminals considerably longer to exploit a vulnerability following its discovery.

To ensure that the right patches are applied at the right time by the right people, organizations should have a patch and maintenance policy in place and do as much as possible to adhere to it at all times.

Why Is This Policy Important?

Even regular computer users with no IT background understand that patches keep software running smoothly and introduce new features. What they sometimes don't fully realize, however, is that patching is one of the most important activities anyone can do to keep cybercriminals at bay.

According to data published by the Ponemon Institute, 57 percent of all data breaches can be directly attributed to attackers exploiting a known vulnerability that hadn't been patched. In most cases, the problem isn't the lack of availability of a patch (only 14 of the nearly 20,000 known software flaws are zero-days) but the lack of an effective patch and maintenance policy.

One doesn't need to look very far to discover just how devastating data breaches caused by unpatched vulnerabilities can be. For example, the massive Equifax breach, which exposed sensitive data of 143 million US consumers, was caused by an Apache Struts vulnerability that had been patched for more than two months.

Worst of all, taking more than two months to patch a critical vulnerability is not unusual at all. In fact, the average time to patch is 102 days, which gives cybercriminals more than enough time to figure out how to exploit the vulnerability for their own selfish gains.

What Does a Patch & Maintenance Policy Include?

A patch and maintenance policy should include all IT assets that cybercriminals could exploit to infiltrate the target organization. Such assets include endpoints (laptops, desktop computers, mobile devices, point-of-sale systems), servers, networking equipment, and all software running on these and other devices.

Here are the main activities that should be covered in a patch and maintenance policy:

- **Monitoring:** It's important to specify who is responsible for monitoring security mailing lists and vendor notifications to learn about new vulnerabilities and patches. Monitoring should also include periodic vulnerability scanning to proactively inspect the potential points of exploitation.
- **Evaluation:** When a new patch becomes available, it should be evaluated and categorized according to its priority and impact. Some patches are so critical that they should be installed without any delay regardless of any downtime they might cause, while other patches can wait.
- **Testing:** If possible, it's best to test patches prior to their implementation to assess their functionality and stability. Often, vendors are forced to release rushed patches that contain more bugs than they fix, and, in some cases, such patches may not be worth the trouble.
- **Scheduling:** Patches should never be installed without first notifying all employees affected by them. It's a good idea to install non-critical patches on a regular schedule, preferably during the least busy time of the day.

- **Implementation:** The department or employee responsible for patching should document the implementation for auditing and tracking purposes.
- **Verification:** Each installed patch should be tested to confirm that it hasn't resulted in any adverse effects.

How to Create and Implement a Patch & Maintenance Policy?

When creating a new patch and maintenance policy, it's important to first create a comprehensive inventory of all IT assets, including endpoints, servers, networking equipment, and so on. This process can be at least partially automated with the help of asset management software. Leading asset management software solutions also simplify the categorization of discovered IT assets according to their risk level.

The next step is to decide the conditions under which different categories of IT assets will be patched. For example, public-facing networking equipment should always be patched as soon as possible, but there's no reason to burn the midnight oil just to patch a warehouse computer with no access to the outside world.

Once patch conditions have been decided, it's time to start monitoring for new vulnerabilities and patches. When a new patch becomes available, it should first be tested and then deployed according to the patch and maintenance policy. The entire patch process should be periodically reviewed and updated as necessary to reflect changes in IT assets.

Conclusion

In today's cybersecurity environment, organizations have to be responsible for their own security to maintain a competitive edge. The cybersecurity policies described in this article can be seen as the foundation for a security program capable of identifying, containing, and neutralizing even the most dangerous cyber-attacks. With a security program in place, organizations can effectively take advantage of modern technologies without endangering their customers and business partners.

The initial cost associated with the implementation of cybersecurity policies pales in comparison with the average cost of a data breach and the associated reputation damage.

Over time, organizations with clearly defined, up-to-date cybersecurity policies save money even if they never enter the crosshairs of cybercriminals because their employees and IT staff are able to operate more efficiently.

OSIbeyond®

About

Established in 2004, OSIbeyond is a leading technology services provider specializing in small to medium sized organizations. OSIbeyond's years of experience as an Managed Services Provider (MSP) led to the development of a business unit solely focused on providing cyber security services. In recent years, OSIbeyond identified a gap in the industry between traditional MSPs and Managed Security Service Providers (MSSP).

This gap is between MSPs, who lack expertise in cyber security, and MSSPs, who may have limited experience in real world IT operations as experienced by a typical OSIbeyond client. By leveraging years of experience running efficient IT operations, providing world-class customer service, and technical expertise in the latest technologies, OSIbeyond developed a new Managed Security Services program from the ground up. The program is designed to complement an organization's existing IT resources, both in-house staff or an MSP. Working in partnership with existing IT teams, OSIbeyond's Managed Security Services provides independent, 3rd party checks & balances for your organization's security posture.

www.osibeyond.com