White Paper

Security

Five Steps: How to Defend Your Company Against a Security Breach

MICRO FOCUS

Table of Contents

page

The NIST Framework 2
NIST Part 1: Identify 3
NIST Part 2: Protect 5
NIST Part 3: Detect. 6
NIST Part 4: Respond 7
NIST Part 5: Recover 8

Acting quickly makes a big difference. Companies that take over 30 days to contain a breach pay more than $1 million more than those who are able to shut it down faster.

The enterprise move to the cloud shows no signs of slowing. By 2020, 83 percent of enterprise workloads are expected to be hosted in the cloud.

It's easy to see why. Using the cloud lessens the burden on IT departments, freeing them to develop new products and services (often in the cloud). It gives today's workers the 24/7 access they demand. Cloud services create new efficiencies, drive innovation, and lower costs.

But the cloud also provides new opportunities for another class of people—the cyberthieves who lurk in the dark corners of the web. Attacks are increasing, both in prevalence and disruptive potential. Cyber breaches have almost doubled in the past five years, according to the World Economic Forum, which now lists cyberattacks as third on its list of top global risks.

Without a doubt, cybercrime has become big business. The odds that your company will be breached within the next 24 months are greater than 1 in 4—27.9 percent, to be exact, according to the Ponemon Institute's 2018 Cost of a Data Breach study. By the time you find the problem, fix your systems, notify everybody, and pay fines, you'll be out an average of $3.86 million (in the U.S., it's $7.91 million).

The longer it takes you to discover the breach, the more you'll pay. Once they've wormed their way into your company's systems through phishing, malware, or social engineering, cybercriminals often spend months learning the ins and outs of your databases before they decide what to steal. Then they may exfiltrate data slowly, hoping you won't catch them in the act.

All too often, they get away with it. The mean time it takes companies to identify a breach is 197 days, and it takes them another 69 days to contain it, according to Ponemon.

Acting quickly makes a big difference. Companies that take over 30 days to contain a breach pay more than $1 million more than those who are able to shut it down faster.

Losing money isn't the only problem. A security breach gives your company a serious black eye, scaring off potential investors and alienating customers. Here are just a few of the many high-profile breaches that have occurred in recent years:

- **Equifax:** In 2017, the Social Security numbers of 145.5 million people were hacked—more than 99 percent of the company's customers. Driver's licenses, taxpayer ID cards, passports, and more than 200,000 credit card numbers and expiration dates were scooped up, too. The company's revenue declined 27 percent in just one quarter. It will spend years trying to restore the public trust it has lost.
- **Yahoo:** In 2013, customer accounts were hacked, but the company didn't reveal size of the problem for years. Eventually, it disclosed that all 3 billion of its users were compromised. That bit of information lowered its value by $350 million when it sold itself to Verizon in 2017.

- **SWIFT:** You might have thought the standard international transfer system used by global banks would be safe, but an attack in 2016 proved otherwise. Criminals who hacked into SWIFT stole $81 million from the central bank in Bangladesh and sent the money to the Philippines.
- **Ukraine's power grid:** was shut down in 2015, affecting 30 substations and 230,000 people and revealing it's not always money cybercriminals are after.
- **Wannacry:** This massive 2017 ransomware attack, which may have been launched by a state actor, took advantage of a Microsoft vulnerability to infect more than 300,000 computers in 150 countries. It hit hospitals in the UK, forcing patients to postpone surgeries, and cost companies around the world billions of dollars.

As you can see, today's cyberattacks go far beyond the clumsy early attempts asking people to send money to a Nigerian prince. Because they are so sophisticated and varied and are launched from such a wide variety of platforms, defending against them is a complex endeavor. But if you approach it systematically, it doesn't have to be a herculean effort.

Today's cyberattacks go far beyond the clumsy early attempts asking people to send money to a Nigerian prince. Because they are so sophisticated and varied and are launched from such a wide variety of platforms, defending against them is a complex endeavor. But if you approach it systematically, it doesn't have to be a herculean effort.

The NIST Framework

There are many angles from which to approach cybersecurity. One of the clearest, most comprehensive, most flexible, and most highly-regarded methods we've found is the framework devised by the National Institute of Standards and Technology (NIST).

The NIST framework is simply a voluntary set of best practices developed to help keep organizations safe. It has gained wide acceptance in both the business and government sectors. More than 30 percent of organizations are using the NIST framework, and use is predicted to rise to 50 percent by 2020, according to Gartner. NIST standards are also being adopted by all U.S. federal government agencies.

The NIST framework has five parts, each of which provides a useful lens for evaluating your company's security and making decisions about how to manage it. You may be following some of its suggestions already. The beauty of NIST is that it lays down a solid base for cyber defense. The kind of structure you build on top of the base is up to you.

Here's an overview of the NIST framework and some ways you can to use it to strengthen every facet of your company's defenses against a breach.

For IT departments, correlating each user or thing to each app and company database they can access is not only time-consuming, it's fraught with potential errors that can lead to a breach if an account is compromised.

NIST Part 1: Identify

It comes as no surprise to us that NIST begins its process by asking you to identify your assets. Before you can start protecting your company's information, you need to determine what your valuable assets are, where they are, and who is using them. Then you need to prioritize them and develop a security policy based on the amount of damage that could result if they were accessed by an unauthorized person or thing.

It's crucial to know at all times who your users are and to control what they are allowed to do. At Micro Focus®, we believe identity is the foundation of security.

Discover

Discovering who has access to what is not as easy as it sounds. If you do it manually, your IT team has to spend countless hours looking up which apps and databases each employee, partner, and contractor uses. That means contacting department managers as well as managers of internal and external apps, then compiling the information and constantly keeping it up to date.

Today's businesses use hundreds of apps—the average enterprise uses 91 cloud services for marketing alone. As the internet of things gains traction, a host of new devices and appliances will connect to the cloud for cloud communications and storage. By 2020, there will be 20 billion internet-connected "things," ranging from jet engines and connected cars to thermostats and vending machines, according to Gartner.

For IT departments, correlating each user or thing to each app and company database they can access is not only time-consuming, it's fraught with potential errors that can lead to a breach if an account is compromised.

That's especially true in the case of privileged users—the IT administrators, top executives, and others with access to your company's most important confidential information. Privileged users are highly valued by hackers and are frequent targets of social engineering and phishing attempts. Their accounts require extra monitoring and security measures. It's important to identify them quickly and make them a priority when developing your security policy.

Automate

Automating your identity and access management system—including the provisioning and deprovisioning of all users—is the only effective way to gain control over your important information. Automation gets the job done quickly and ensures that no unauthorized users slip through the cracks.

It produces an accurate picture that takes many companies by surprise. We've worked with enterprises that have discovered thousands of user accounts with access to sensitive information they no longer need. Some have changed job roles and others have left the company entirely.

With an automated system, managers periodically review and approve the access privileges of all current employees. When someone changes roles, the list of programs and databases they are allowed to use is modified accordingly. It's a simple check-off process for them, but it's vital to your company's security health.

If an employee quits or is fired, the system automatically shuts off all their access privileges immediately. With manual systems, it sometimes takes two or three days for administrators to catch up.

A disgruntled former employee can wreak havoc, as Coca-Cola recently learned after a fired employee stole the personal information of 8,000 workers. Information like this is valuable on the dark web where cybercriminals ply their trade. Using valid employee credentials, a hacker can log onto a corporate site undetected, then try to escalate access privileges to breach sensitive financial and customer information.

Not all problem accounts belong to people. Most companies also have service accounts, which are operated by web servers or databases to make changes to system configurations. They should be disabled after completing their tasks, but many slip through the cracks.

Service accounts are ideal portals for hackers. No one pays attention to them, making them a comfortable, shady spot to lurk while casing the business. Some have enough access to high-level information to be classified as privileged accounts, making it even more critical for you to identify them and shut them down as soon as possible.

Service accounts are ideal portals for hackers. No one pays attention to them, making them a comfortable, shady spot to lurk while casing the business. Some have enough access to high-level information to be classified as privileged accounts, making it even more critical for you to identify them and shut them down as soon as possible.

Set a Policy

Doing an automated access audit will help you cut off unauthorized accounts you didn't know existed and reduce the access privileges of many more. After that, you will need to take a hard look at what's left and follow the "least privilege" principle, giving people (and things) access only to the tools they need to do their jobs—no more and no less.

Codify your access rules in a centrally-managed governance policy and use automation to ensure that they're enforced at all times across all users and devices, including partners and contractors with whom you share information.

Creating a robust identity and access management system may sound like a tall order. But with automation, you can do it relatively quickly and keep it updated painlessly as users and roles change and your company scales. It will serve as the foundation for everything else you do to keep bad external and internal actors out.

Adapting authentication requirements to the situation gives users the best experience possible while maintaining rigorous security for your data

NIST Part 2: Protect

Once you've set up a strong governance policy based on users and roles, you need to enforce it. Even though you now have an up-to-date list correlating users to devices and work locations, you need to do more. Today's employees may sign onto your applications from home, a coffee shop, an airport, or a foreign country. How can you be sure they are who they say they are?

Authenticate Your Users

In addition to asking for a username and password, you may require a second or third form of identification to allow users in, even if their roles normally entitle them to the information they're seeking. Multifactor authentication comes in many forms, including text messages, tokens, and biometric data such as a fingerprint or facial recognition.

Access decisions are always a balancing act. Requiring users to jump through too many hoops frustrates them and lowers productivity. On the other hand, loosening controls too much could result in a breach. That's why Micro Focus recommends using an adaptive authentication system.

An adaptive system allows you to step up access requirements depending on the user, time, place, and circumstances. If a worker based in Cleveland tries to sign in from Beijing, the system may require a second factor. If she tries to do something out of the norm—such as downloading your customer database—it will require even more identification—or perhaps shut off access completely until your security team can determine whether the request is legitimate.

Adapting authentication requirements to the situation gives users the best experience possible while maintaining rigorous security for your data.

Encrypt Sensitive Data

Your most confidential data—financials, patented and trademarked processes, personally-identifiable customer and employee information, and anything covered by regulations such as HIPAA or FINRA—requires even more protection. This data should be encrypted every time it is transmitted, and only authorized users should be allowed to decrypt it.

You should also encrypt the bodies of emails to which the information is attached, since they may discuss some of its particulars.

Keep Systems and Programs Updated

Operating systems and applications are updated over time, and not all of the changes are product improvements. Many updates are created to patch security holes, sometimes after cyberthieves have already discovered them.

Ignoring security updates or rolling them out too slowly is perilous. Equifax could have avoided the disastrous theft of over 145 million Social Security numbers if it had fixed a known vulnerability in the Apache Struts web framework sooner than it did. Organizations across Europe would never have been hit by the Wannacry ransomware attack if they had patched or moved to an updated version of the Microsoft operating system.

Centralized management, timely updates, and virtualization are some of the practices you can use to stay ahead of the latest security threats.

Keep Users Informed

No matter how tight your security policy is, your users can subvert it through carelessness, ignorance, or a lack of concern. You should conduct regular security training sessions to inform them of the latest threats and remind them of the potential consequences of engaging in risky behavior such as sharing passwords.

NIST Part 3: Detect

Despite your best efforts at protection, your systems may be compromised by hackers, who constantly hone their tactics to exploit vulnerabilities. And you never know when an employee or contractor might decide to go rogue. Even well-intentioned people may be introducing security holes as they write new code.

Monitor Your Systems

To protect your systems and assets, you need an ongoing monitoring system that watches all activity and detects anomalies in real time. You should monitor data from hosts, applications, network devices, databases, and users. The more information you have, the sharper your analysis will be.

After a data breach, analysis of the audit log often reveals clear evidence of malicious activity. If the threats could have been detected earlier, the breach would not have occurred.

Security and event monitoring technology uses machine learning to gain a sense of normal activity at your organization. If suspicious activity occurs—such as changing, deleting, or exporting sensitive information—it will alert security officers immediately.

Monitor Your Privileged Users

You should also monitor the sessions of privileged users whenever they access sensitive information. Even if you trust these people, monitoring is essential.

It's possible for a hacker to execute code to elevate their privileges and impersonate someone else. According to Forrester, 80 percent of breaches involve privileged accounts. A monitoring system records every keystroke they make while they're handling your most critical assets.

You should also monitor the sessions of privileged users whenever they access sensitive information. Even if you trust these people, monitoring is essential.

Micro Focus has a system that monitors all privileged activity behind the scenes, so privileged users don't have to log onto a separate portal several times a day to do their jobs.

You should also configure your system to automatically change privileged users' passwords every time they log off a sensitive database. Privileged users should never be allowed to share passwords. Everything they do requires extra caution because of the value of the information they handle and their attractiveness to hackers.

Users with access to high-level information usually understand the need for security precautions, but repeated logins and authentication procedures can be demoralizing and interfere with their work processes. Micro Focus has a system that monitors all privileged activity behind the scenes, so privileged users don't have to log onto a separate portal several times a day to do their jobs.

However you do it, you need to have a system in place to keep privileged accounts in check at all times.

Scan Your Code

In addition to scanning all your existing applications for exploit attempts, you should monitor the new code your developers are writing as they create applications.

Programmers make mistakes all the time—it's part of the development process. But you don't want bugs that serve as a back door to your valuable information.

It's a good idea to use software to scan code as it's being written for patterns indicating errors that cause security problems. As new products are completed, you can do penetration testing to make sure they behave as expected and don't create a security hole.

NIST Part 4: Respond

Hackers thrive on organizational chaos. Systematic controls can help you stop an incipient breach or limit the amount of damage it can do.

Develop a Plan

A good security plan creates responses in advance to a variety of threats, ensuring quick reaction times and orderly communication to appropriate authorities. Test your plan, track response times, and analyze your procedures to see if efficiency can be improved.

Correlate Events

An effective monitoring system not only scans your network for anomalies, it correlates events to determine whether a problem warrants immediate attention.

If you experience a spike in network traffic, it could be because customers are responding to a special deal or a viral blog post. But if the traffic spike happens in conjunction with an elevated number of failed login attempts, someone may be initiating a denial of service attack on your website—deluging it with so much traffic that it's forced to shut down.

Cyber criminals sometimes launch these attacks to distract the IT department while they stage a second attack to fulfil their real goal—exfiltrating data or damaging your systems.

Cyber criminals sometimes launch these attacks to distract the IT department while they stage a second attack to fulfil their real goal—exfiltrating data or damaging your systems.

Determine the Best Course of Action

You need to respond quickly, but shutting down everything would cost you money and customers. Instead, you can set your system to isolate and quarantine only the part of the network that's affected. That prevents further damage and allows the rest of the business to continue operating as usual.

It also allows your security analysts to watch the cybercriminal, who is unaware that you have constrained his ability to do harm. By watching his methodology, they may learn more about him and find out where he came from. What they discover could prevent the attacker from coming back through a different vector. They may also discover and close an application vulnerability or find a user account that has been compromised and terminate its access.

NIST Part 5: Recover

Part of your cybersecurity plan should include a means of restoring any systems and data affected by a breach while impacting the business as little as possible. Your servers and data should all have backups to enable you to get up and running again quickly.

While its lessons are painful, a breach can lead you to improve your controls and detection in the future. Probe your network for weaknesses and update or replace old software that could lead to problems. Reexamine your security policies and procedures in light of the incident and other current threats.

A robust security system has layers of defenses. If one filter misses something, another one can catch it. You may want to bring in an unbiassed third party to analyze what went wrong and find gaps that your security team may be unaware of.

Micro Focus Can Help

Whether you've already experienced a breach or want to do your best to avoid one, Micro Focus can help. We have aligned our systems with NIST's framework to address all of the complex security challenges today's environment brings.

Our solutions are guided by over 10 years' experience, and our 1,200 security professionals operate in 120 countries. Nine out of 10 global payment processors trust our system to handle their transactions.

Our approach is to perform a security assessment that examines your people, processes, technology, and business priorities to determine what kind of security infrastructure is right for you.

Unlike other companies, we are happy to work with the vendors and technology you already have in place. We have a comprehensive set of solutions, but we don't insist that you use them all. Our goal is to address your individual needs. We will make the old work with the new, bringing you up to speed with the latest security advancements while increasing the value of your previous investments.

Our solutions are guided by over 10 years' experience, and our 1,200 security professionals operate in 120 countries. Nine out of 10 global payment processors trust our system to handle their transactions.

We've worked with governments and enterprises in industries ranging from technology and banking to retail, healthcare, education, entertainment, and many others. We can help you with security and compliance no matter what kind of regulations you need to follow.

To learn more about strengthening your company's security to defend against a costly breach, contact [sales rep] today.

Contact your Zones Account Manager at
800.408.9663, or visit zones.com, for more details.

ZONES
First Choice for IT™

MICRO FOCUS