Basic Security Concepts

(Definitions are in the notes)

Difference between vulnerabilities and threats

* Vulnerability exposes organisations to threats

A threat is a person or event that has the potential for impacting a valuable resource in a negative manner. A vulnerability is that quality of a resource or its environment that allows the threat to be realized. An armed bank robber is an example of a threat.

**Vulnerability**

* Network Vulnerabilities. These are issues with a network’s hardware or software that expose it to possible intrusion by an outside party. Examples include insecure Wi-Fi access points and poorly-configured firewalls.
* Operating System Vulnerabilities. These are vulnerabilities within a particular operating system that hackers may exploit to gain access to an asset the OS is installed on—or to cause damage. Examples include default superuser accounts that may exist in some OS installs and hidden backdoor programs.
* Human Vulnerabilities. The weakest link in many cybersecurity architectures is the human element. User errors can easily expose sensitive data, create exploitable access points for attackers, or disrupt systems.
* Process Vulnerabilities. Some vulnerabilities can be created by specific process controls (or a lack thereof). One example would be the use of weak passwords (which may also fall under human vulnerabilities).

Examples of vulnerabilities

User-based Vulnerability

Admin-based Vulnerability

Eg. Privilege allocation

Causes of vulnerabilities

* Complex Systems – ‍Complex systems increase the probability of misconfigurations, flaws, or unintended access.
* Familiarity – Attackers may be familiar with common code, operating systems, hardware, and software that lead to known vulnerabilities.
* Connectivity – ‍Connected devices are more prone to have vulnerabilities.
* Poor Password Management – ‍Weak and reused passwords can lead from one data breach to several.
* OS Flaws – ‍Operating systems can have flaws too. Unsecured operating systems by default can give users full access and become a target for viruses and malware.‍
* Internet – ‍The internet is full of spyware and adware that can be installed automatically on computers.
* Software Bugs – Programmers can sometimes accidentally, leave an exploitable bug in the software.
* Unchecked user input – ‍If software or a website assumes that all input is safe, it may run unintended SQL injection.
* People – Social engineering is the biggest threat to the majority of organizations. So, humans can be one of the biggest causes of vulnerability.

Common vulnerabilities

**1. Misconfigurations**

Misconfigurations are the single largest threat to both cloud and app security. Because many application security tools require manual configuration, this process can be rife with errors and take considerable time to manage and update.

In recent years, numerous publicly reported breaches started with misconfigured S3 buckets that were used as the entry point. These errors transform cloud workloads into obvious targets that can be easily discovered with a simple web crawler. The absence of perimeter security within the cloud further compounds the risk associated with misconfigurations.

To that end, it is important for organizations to adopt security tooling and technologies and automate the configuration process and reduce the risk of human error within the IT environment.

**2. Unsecured APIs**

Another common security vulnerability is unsecured application programming interfaces (APIs). APIs provide a digital interface that enables applications or components of applications to communicate with each other over the internet or via a private network.

APIs are one of the few organizational assets with a public IP address. If not properly and adequately secured, they can become an easy target for attackers to breach.

As with misconfigurations, securing APIs is a process prone to human error. While rarely malicious, IT teams may simply be unaware of the unique security risk this asset possesses and rely on standard security controls. Conducting a security awareness training to educate teams on security best practices specific to the cloud — such as how to store secrets, how to rotate keys and how to practice good IT hygiene during software development — is critical in the cloud, just as in a traditional environment.

**3. Outdated or Unpatched Software**

Software vendors periodically release application updates to either add new features and functionalities or patch known cybersecurity vulnerabilities. Unpatched or outdated software often make for an easy target for advanced cybercriminals. As with system misconfigurations, adversaries are on the prowl for such weaknesses that can be exploited.

While software updates may contain valuable and important security measures, it is the responsibility of the organization to update their network and all endpoints.

Unfortunately, because updates from different software applications can be released daily and IT teams are typically overburdened, it can be easy to fall behind on updates and patching, or miss a new release entirely. Failing to update even one machine can have potentially disastrous consequences for the organization, providing an attack path for ransomware, malware and a host of other security threats

To help address this issue, organizations should develop and implement a process for prioritizing software updates and patching. To the extent possible, the team should also automate this activity so as to ensure systems and endpoints are as up to date and secure as possible.

**4. Zero-day Vulnerabilities**

A zero-day vulnerability refers to a security flaw that has been discovered by a threat actor but is unknown to the enterprise and software vendor. The term “zero-day” is used because the software vendor was unaware of their software vulnerability, and they’ve had “0” days to work on a security patch or an update to fix the issue; meanwhile it is a known vulnerability to the attacker.

Zero-day attacks are extremely dangerous for companies because they can be very difficult to detect. To effectively detect and mitigate zero-day attacks, a coordinated defense is needed — one that includes both prevention technology and a thorough response plan in the event of a cyberattack. Organizations can prepare for these stealthy and damaging events by deploying a complete endpoint security solution that combines technologies including next-gen antivirus (NGAV), endpoint detection and response (EDR) and threat intelligence.

**5. Weak or Stolen User Credentials**

Many users fail to create unique and strong passwords for each of their accounts. Reusing or recycling passwords and user IDs creates another potential avenue of exploitation for cybercriminals.

Weak user credentials are most often exploited in brute force attacks when a threat actor tries to gain unauthorized access to sensitive data and systems by systematically trying as many combinations of usernames and guessed passwords as possible. If successful, the actor can enter the system and masquerade as the legitimate user; the adversary can use this time to move laterally, install back doors, gain knowledge about the system to use in future cyberattacks, and, of course, steal data.

To address this particular cybersecurity vulnerability, organizations should set and enforce clear policies that require the use of strong, unique passwords and prompt users to change them regularly. Organizations should also consider implementing a multifactor authentication (MFA) policy, which requires more than one form of identification, such as both a password and a fingerprint or a password and a one-time security token, to authenticate the user.

**6. Access Control or Unauthorized Access**

Companies often grant employees more access and permissions than needed to perform their job functions. This increases identity-based threats and expands access to adversaries in the event of a data breach.

To address this issue, organizations should implement the principle of least privilege (POLP), a computer security concept and practice that gives users limited access rights based on the tasks necessary to their job. POLP ensures only authorized users whose identity has been verified have the necessary permissions to execute jobs within certain systems, applications, data and other assets.

POLP is widely considered to be one of the most effective practices for strengthening the organization’s cybersecurity posture, in that it allows organizations to control and monitor network and data access.

**7. Misunderstanding the “Shared Responsibility Model” (i.e., Runtime Threats)**

Cloud networks adhere to what is known as the “shared responsibility model.” This means that much of the underlying infrastructure is secured by the cloud service provider. However, the organization is responsible for everything else, including the operating system, applications and data.

Unfortunately, this point can be misunderstood, leading to the assumption that cloud workloads are fully protected by the cloud provider. This results in users unknowingly running workloads in a public cloud that are not fully protected, meaning adversaries can target the operating system and the applications to obtain access.

Organizations that are using the cloud or shifting to a cloud or hybrid work environment must update their cybersecurity strategy and tooling to ensure they are protecting all areas of risk across all environments. Traditional security measures do not provide security in a cloud environment and must be supplemented to provide enhanced protection from cloud-based vulnerabilities and threats.

Vulnerability Solutions

**Managing exposure to known cybersecurity vulnerabilities** is the primary responsibility of a vulnerability manager. Although vulnerability management involves more than simply running a scanning tool, a high-quality vulnerability tool or toolset can dramatically improve the implementation and ongoing success of a vulnerability management program.

The market is filled with options and solutions, each claiming leading qualities. When evaluating a vulnerability management solution, keep these things in mind:

**Timeliness is important.** If a vulnerability management tool fails to detect vulnerabilities in a timely manner, then the tool isn’t very useful and doesn’t contribute to overall protection. This is where network-based scanners often fail. It can take a long time to complete a scan and consume a large portion of your organization’s valuable bandwidth only to produce immediately outdated information. It’s better to choose a solution that relies on a lightweight agent rather than on a network.

**Performance impact on an endpoint is key**. Increasingly, vulnerability scanning vendors claim to offer agent-based solutions. Unfortunately, most of these agents are so bulky that they dramatically impact an endpoint’s performance. Therefore, when searching for an agent-based tool, look for one with a lightweight agent — one that consumes very little space on an endpoint to minimize any effect on productivity.

**Real-time, comprehensive visibility is critical.** You should be able to see what’s vulnerable in an instant. Legacy vulnerability tools can hinder visibility — network scans take a long time and provide outdated results, bloated agents slow business productivity, and bulky reports do little to help address security vulnerabilities in a timely manner.

**Less is more.** Organizations no longer need a complicated set of security tools and solutions that require personnel with specialized skills. Instead, many now rely on an integrated platform that includes vulnerability management tools along with other security tools for cyber hygiene, endpoint detection and response, device control and more — ultimately protecting your organization from attack due to unprotected systems.

**Threat**

Examples of threats

**1. Malware**

Malware is malicious software, including viruses and worms, injected into networks and systems with the intention of causing disruption. Malware can extract confidential information, deny service and gain access to systems.

IT departments use antivirus software and firewalls to monitor and intercept malware before it gains entry to networks and systems, but bad actors continue to evolve their malware to elude these defenses. That makes maintaining current updates to security software and firewalls essential. There are also hardware solutions for thwarting malware, such as Gryphon’s Guardian mesh router, which handles a variety of threats.

**2. Ransomware**

Ransomware is a type of malware. It blocks access to a system or threatens to publish proprietary information. Ransomware perpetrators demand that their victims’ companies pay them cash ransoms to unlock systems or return information.

So far in 2022, ransomware attacks on companies are 33% higher than they were in 2021. Many companies agree to pay ransoms to get their systems back only to be hit again by the same ransomware perpetrators.

Rob Floretta, cybersecurity manager for a large utility provider, warned that bad actors, whether they are deploying malware, spyware, exfiltrating valuable data or deploying other varieties of attack, can hide within a company’s network. Reducing their dwell time “inside” corporate systems is key.

“Dwell time is how long someone lives off your land before you detect them,” he said. “That has dropped significantly in recent years but there is still work to be done.”

Mandiant reported that global median dwell time for intrusions identified by external third parties and disclosed to the victims dropped to 28 days from 73 days in 2020. Meanwhile, in 2021, 55% of investigations had dwell times of 30 days or fewer, with 67% of these (37% of total intrusions) being discovered in one week or less. However, the report also showed that supply chain compromise accounted for 17% of intrusions in 2021 compared to less than 1% in 2020.

**3. Supply chain vulnerabilities**

Supply chain hacks, which include the infamous SolarWinds attack that found its way to several government agencies and perhaps lesser known exploits involving JS.node vulnerabilities, are especially pernicious because the size of the threat surface is basically wherever tainted software goes.

In the case of SolarWinds’ Orion update, that surface included hundreds of consulting, technology, telecom and extractive entities in North America, Europe, Asia and the Middle East.

One step companies can take is to audit the security measures that their suppliers and vendors use to ensure that the end-to-end supply chain is secure.

Justin Cappos, a professor of computer science at NYU who created the open-source security protocol called in-toto, explained that people typically rely SBOM (software bill of materials) to “know” what’s in their software supply chain.

“These are a little like nutrition labels on food,” he explained. “If you can’t attest to the accuracy of these labels, you have a problem. That’s where things like in-toto come in: You create essentially signed statements, or attestations, that certain people, and only those people, took legitimate actions like checking code or doing things with dependencies.”

**4. Phishing**

Software can do only so much to defend against social engineering. Almost everyone has received a suspicious email — or worse yet, an email that appears to be legitimate and from a trusted party but isn’t. This email trickery is known as phishing.

Phishing is a major threat to companies because it’s easy for unsuspecting employees to open bogus emails and unleash viruses. Employee training on how to recognize phony emails, report them and never open them can really help. IT should team with HR to ensure that sound email habits are taught.

There are many vendors who offer training and packaged solutions for companies looking for something approaching a turnkey solution. There are also tech solutions.

Cappos said password managers are a critical first line of defense.

“There’s never any reason why you should ever share a verification code with anyone,” he said. “You should use authenticator apps, and not ones that send you a text message.”

He also noted that Android and iPhone have improved protective measures, such as lockdown mode on iPhone and features in the open-source GrapheneOS for Pixel.

**5. IoT**

In 2020, 61% of companies were using IoT, and this percentage only continues to increase. With the expansion of IoT, security risks also grow, particularly with the advent of 5G telecommunications, the de facto communications network for connected devices.

IoT vendors are notorious for implementing little to no security on their devices, a threat that can be ameliorated through stronger vetting of IoT vendors upfront in the RFP process for security and by resetting IoT security defaults on devices so they conform to corporate standards.

SEE: A brief history of industrial IoT (TechRepublic)

“IoT devices generally contain simple-to-guess credentials, or their default passwords are readily available on the internet,” Floretta said. “Following simple cybersecurity best practices, such as changing passwords after installation, will make it much more difficult for compromise by bad actors.”

If your organization is looking for more guidance on IoT security, the experts at TechRepublic Premium have put together an ebook for IT leaders that is filled with what to look out for and strategies to deal with threats.

**6. Internal employees**

Disgruntled employees can sabotage networks or make off with intellectual property and proprietary information, and employees who practice poor security habits can inadvertently share passwords and leave equipment unprotected. This is why there has been an uptick in the number of companies that use social engineering audits to check how well employee security policies and procedures are working.

In 2023, social engineering audits will continue to be used so IT can check the robustness of its workforce security policies and practices.

**7. Data poisoning**

An IBM 2022 study found that 35% of companies were using AI in their business and 42% were exploring it. Artificial intelligence is going to open up new possibilities for companies in every industry. Unfortunately, the bad actors know this too.

One need look no further than the Log4J Log4Shell bug for proof that data poisoning in AI systems is ascendant. In a data poisoning, a malicious actor finds a way to inject corrupted data into an AI system that will skew the results of an AI inquiry, potentially returning an AI result to company decision makers that is false.

Data poisoning is a new attack vector into corporate systems. One way to protect against it is to continuously monitor your AI results. If you suddenly see a system trending significantly away from what it has revealed in the past, it’s time to look at the integrity of the data.

**8. New technology**

Organizations are adopting new technology like biometrics. These technologies yield enormous benefits, but they also introduce new security risks since IT has limited experience with them. One step IT can take is to carefully vet each new technology and its vendors before signing a purchase agreement.

“Biometrics encompasses a range of technologies: It could be voice, retinal scanning and even behavior,” said Floretta.

A major benefit is that some biometrics are immutable, unlike passwords.

Contextual authentication (or adaptive authentication) is a behavior-based authentication, the essence of which is: “I’m pretty sure I know who you are based on your behavior, but if I’m seeing something not normal for you, I need to act.”

**9. Multi-layer security**

How much security is enough? If you’ve firewalled your network, installed security monitoring and interception software, secured your servers, issued multi-factor identification sign-ons to employees and implemented data encryption, but you forgot to lock physical facilities containing servers or to install the latest security updates on smartphones, are you covered?

There are many layers of security that IT must batten down and monitor. IT can tighten up security by creating a checklist for every security breach point in a workflow.

SEE: Two-factor authentication evaluation guide (TechRepublic Academy)

“Multiple levels of defense are critical,” said Ed Amoroso, CEO of TAGCyber and former CISO of AT&T. “Passwords are one critical layer, but data encryption at both ends is the next, and so forth. The bottom line: Just because you got in doesn’t mean I trust you. The only barrier to multiple layers of security, frankly, is just cost.”

**10. Cloud security**

Yes, the 2019 data breach by a Seattle hacker resulted in the theft of some 100 million credit applications, but the exfiltration of a misconfigured AWS storage bucket in the cloud led to something else — regulatory headaches for the company.

Potential fines from the regulatory oversight of containers is, paradoxically, one of the major cyber challenges experts are pointing to for 2023. When it comes to corporate reputation and pocketbook, the blowback could be as bad as the break-in.

In the above case, a federal court found Capital One negligent for failing to secure financial data. That came with an $80 million fine, plus customer lawsuits for $190 million.

“There is risk for companies if they are not doing their configuration management and tracking their regulatory compliance they are required to follow,” said Kayne Mcgladrey, field CISO for Hyperproof and a senior member of the IEEE.

He explained that modern cybersecurity and associated regulatory frameworks require data encryption at rest and in transit.

“If companies are encrypting, it’s an easy day, and there’s no problem,” he said. “The real risk I’m starting to see in such vendor negotiations as B-to-B purchasing agreements is that companies want an attestation that the [vendor] is monitoring encryption of all their cloud storage. Companies are asking one another: Can you verify, and do you regularly check that your cloud storage is encrypted?”

From a technology perspective, that’s fairly easy to do, but as Mcgladrey noted, anybody in an organization who has permissions on cloud computing platforms like AWS, Microsoft Azure or Google Cloud can stand up a storage bucket. They can create a storage location in the cloud, but they don’t necessarily have to encrypt them.

“Out of all the CISO’s and security leaders I’ve spoken with over the last three months, the main theme of 2023 is going to be ‘the year of risk,’ and a lot of that risk we’re talking about at this level is regulatory,” said Mcgladrey.

**Risk**

**Countermeasure**

**Incident**

**Trust**