riverbed

Guide

Today's Security Threats and How to Combat them

Hardly a week goes by when there is not news of a cyber-attack on a global organization. As hackers become more sophisticated, they are developing new ways to break down protective barriers, steal data and company secrets, and wreak havoc on organizations around the world.

This paper will not only detail the different types of security threats organizations face today, it will also help you understand how network security analytics can work in conjunction with other tools to combat them. It will cover:

1. The three classes of attacks: availability, confidentiality, and integrity
2. The impetus for attacks and why attackers target certain organizations
3. The different types of attacks, from DDoS to data leakage
4. How to defend against attacks

To successfully defend your company, you need to understand the reasoning and strategy behind an attack, and how and where you might be vulnerable. Only then can you effectively protect yourself.

Classes of Attacks

The cybercrime landscape is not only vast it is constantly evolving. Looking at the landscape overall, there are three major areas of attack: availability, confidentiality and integrity. Sometimes organizations are vulnerable to all three kinds of attacks, and other times just one. Regardless, it is important to understand the different types of threats.

1. Availability

Availability attacks focus on making an organization's service unavailable for a period. The more significant the attack, the longer the downtime. For instance, perpetrators might bring an online retailer's website down on Black Friday, or take a bank offline so it can't service its online service customers.

While nearly every organization is dependent on the Internet in some way, those with heavy Web services components or that rely on internal network services are most vulnerable. DDoS attacks tend to be the most common availability attack.

2. Confidentiality Attack

Confidentiality attacks can be very damaging because they are concerned with stealing confidential information—customer credit card numbers, company secrets, or other sensitive data that organizations protect for a reason. Espionage and data breaches are the result of confidentiality attacks because they focus on stealing private information. Even organizations like the NSA, Staples, the U.S. Postal Service, Morgan Stanley and Sony have been victims of confidentiality attacks.

Social engineering, malicious insiders, compromised credentials and other vectors are the "weapons" that are often used in confidentiality attacks.

3. Integrity Attack

Integrity attacks focus on tarnishing an organization's reputation by modifying data that publicly humiliates the company. The idea is to rewrite existing copy so it can no longer be trusted. News organizations are particularly vulnerable to integrity attacks because their business depends on honest reporting. Similarly, government organizations such as the Centers for Disease Control are also susceptible since a perpetrator might want to cause panic by creating false information about a deadly disease, for example.

Any organization's integrity can be compromised using social engineering, malware or website defacement to damage the trust in an organization because it becomes unclear what information is true and what is fabricated.

Impetus for an Attack

To defend yourself from a network attack, you first need to understand what assets you have: your vulnerabilities: and why someone might attack you.

Your assets

You need to take a hard look at what you own that someone else may want, and then protect it as if it is in Fort Knox.

- What do you own that others want to steal or deface?
- Customer data?
- Product formulas?
- Security codes?
- Intellectual property?
- Trusted access to third-party resources?

Your vulnerabilities

Attackers always look for a weakness they can exploit. If you are an online retailer like Amazon.com or Zappos.com, you cannot do business without your website. You are very vulnerable to an availability attack.

If you are an intelligence agency, government contractor or financial institution with top-secret information, you are susceptible to a confidentiality attack.

If you are a news agency or government organization, you are vulnerable to an integrity attack.

Assess your situation and determine your most desirable assets and your resulting vulnerabilities. Understanding your vulnerabilities is a good step toward creating a strong defense.

Why attacks happen

Once you have figured out what is at risk, you need to determine why an attacker would target your organization. This can be looked at three different ways: means, motive and opportunity.

1. **Means:** You are at risk of attack if someone has the means. Maybe they have swiped a key access card, hacked into your network, or developed a network of botnets (a.k.a. zombies) because they have access to thousands of computers and technology. Essentially, if people have the means to access and the malicious intent, they will find the opportunity to either steal it or destroy it.

2. **Motive:** In any crime, there is always a motive. In the case of cybercrimes, the motive is usually one of the following that can be remembered with the acronym MICE—monetary gain, ideology, coercion, or ego. You can narrow down what type of perpetrator you are looking at based on motive.

- **Monetary gain:** When someone is being paid to launch an attack, demands a ransom, steals information that translates into monetary profit (e.g., credit card theft), or stands to make money from some other organization's downfall, money is the motive.
- **Ideology:** Attacks are sometimes ideological. Someone or some group is angry at an organization for political, religious, environmental, or social reasons and wants it to suffer consequences. They might disagree with specific beliefs, want to make a statement, raise awareness for their opinions, or simply destroy someone else's beliefs.

- **Coercion:** Sometimes attackers are not personally motivated but are coerced by another organization or individual. For instance, a competitor, politician or state actor may not have the skills themselves, so they pressure someone else into doing their dirty work.
- **Ego:** Sometimes attacks come down to ego and are a twisted way of making someone feel important. Attacks can feed the ego by "proving" their power and influence—e.g., "I'm smarter than you are because I can deface your website and tarnish your brand."

3. **Opportunity:** To launch an attack, someone must have the opportunity. Hacking into computers is much easier than breaking down brick walls, but you still need an entry point. Because computers are connected via the Internet, someone who knows what they are doing can get in. Edward Snowden had the opportunity to access information because he was trusted by the NSA and no one was watching him—sometimes that's all it takes.

In the end, you can narrow down what type of perpetrator(s) you are looking at by analyzing their approach. Defending your assets is the next step. You can't just invest in network security analytics then set it and forget it. Your network security defenses are like tanks and airplanes; someone must choose which one is going to be most effective against a threat.

Types of Attacks

It is important to understand the different types of threats so you can build appropriate defenses against them.

DDoS attacks

The goal of DDoS attacks is downtime—to bring down an organization's website and halt or slow business by creating a surge of unauthorized traffic that chokes the system. To stage a DDoS attack, you need thousands of computers that overwhelm the website. One way to acquire these computers is through phishing scams where perpetrators try to get innocent people to click without realizing that malware is being launched in the background, compromising their systems.

Brute force attacks

Rather than exploit weaknesses in software, these attacks are much simpler—they focus on breaking down barriers by trying to decipher a login and password. Computers usually try up to 15,000 passwords before they give up and move onto another machine. If you are monitoring your network and you see this kind of activity, it is likely that you're the target of a brute force attack.

Malware

Worms, Trojan horses, viruses, spyware and other malicious software are all considered types of malware. These hostile programs are a means to an end—data theft, espionage or sabotage. While malware is typically very damaging to systems and networks, the number of attacks has steadily decreased over the past few years because systems are being built better and are harder to penetrate; but it is still a threat.

Social engineering

When cybercriminals exploit human weaknesses by psychologically manipulating them into providing system access or divulging confidential information, this is social engineering. Phishing is a common form of social engineering. It's used to infect computers by exploiting the notion that people are trusting and will open emails they shouldn't, unknowingly infecting their computers.

Data exfiltration

Data exfiltration occurs when confidential data gets leaked, either through malicious intent or inadvertently. Detecting data breaches and exfiltration transmission is critical because sensitive data, such as financial, patient data, credit card information, and intellectual property, can cripple an organization and its brand if it gets out.

Defending Your Network

Once you understand where your organization might be vulnerable, why someone might want to attack you, and what approach they will likely use, how do you defend yourself?

Visibility

Network security analytics is more than just a window into your network; it is insight. It allows you to see what normal activity looks like so you can detect changes in behavior. For example, the average individual writes and sends about 30-50 emails a day. Visibility into your network means you can see when someone sends 1,000 emails, which serves as a warning sign because it is out of the norm.

Similarly, desktop computers typically talk to about 400 other computers every day, so a significant increase is flagged as anomalous.

These days, attackers have become smarter and commonly encrypt their communications, which is harder to detect and defend against. Nevertheless, visibility into anomalous behavior—behavior that is unusual—provides insight into what is happening.

Defenses

Any type of defense is better than nothing at all, but understanding why you might be a target will help you customize your defense strategy most effectively.

Computers today have millions more files than in the past, making it easier for attackers to hide. When it comes to defending your network in a cost-effective way, you may have to lure the attackers out. The moment the attacker communicates over the network is when you stand a chance of catching him. With network security analytics, you are able to catch hackers in the act.

Conclusion

While the real intelligence starts with human beings who understand where and why someone might attack them and set up an appropriate defense, network security analytics are also essential for fending off attackers. These high-speed visibility tools can handle significant volumes of network information that would be difficult to digest by even a super human.

To fend off cyberattacks, your organization needs both network analysis tools and a dedicated individual who can make actionable and intelligent decisions on the fly. It will make all the difference in the end.

To learn more about how Riverbed® NPM can help you identify and defend against today's security threats quickly, click here.