Threat Hunting for Cybersecurity Defense

Using threat hunting as part of a cybersecurity defense plan can help you identify attackers, their tactics, and their goals which allows for continuous improvement of security. It can also help you understand the trends in your security environment. This article will outline how to conduct threat hunting, how to identify threats, and how to defend against possible threats.

What is Threat Hunting

Threat hunting is actively seeking indicators of potential cyber incidents that could adversely affect your company. A threat hunt could take many different turns and result in days of hunting following many different paths. Threat hunting is never a singular process, you need to be continuously hunting for a variety of threats and trying to predict potential cyber threats to your business.

Identifying & Defending Against Threats

The Internet has evolved dramatically. As a result, it has become a critical communications infrastructure. It is also a target of advanced adversaries, who continually develop and use malicious techniques. Therefore, threat hunters must be aware of and stay on top of quickly changing software and infrastructure. You are only able to defend against a threat if you’re able to identify them. Being able to identify threats requires you to have adequate threat intelligence, in-depth knowledge of your network, ongoing security testing, and proper procedures and technology in place. With these defenses

in place you gain knowledge that allows you to determine which activity is potentially malicious and which activity is normal. Only with this in place are you able to identify and defend against threats.

Potential Indicators of a threat include:

- Spear Phishing
- Multiple Failed log-in attempts
- Somebody downloading massive amounts of company files
- Program or user attempting to gain access to unauthorized areas

Conducting a Threat Hunt

Conducting a threat hunt is not an easy 3 step process as it takes a lot of preparation learning and observing before the threat hunt process can even begin. Identifying and collecting information about an attacker's tactics, methods, and goals are critical to cybersecurity defense. If you don't have some background knowledge of how cyber criminals work, it's incredibly difficult to predict their next move. Also, information gathered at this stage can be used to gather details about an organization, such as who has access to specific information and how that information is being used. After obtaining background knowledge then you're ready to begin the first step in threat hunting.

1. The first step in threat hunting is knowing what you're looking for. For example, you want to make sure there is no unauthorized access within your network. You can then use threat intelligence and your own prior knowledge to hypothesize how a cyber criminal may achieve gaining access to your network.

2. After hypothesizing, you then need to gather as much

information as you can. Information is collected in various ways, including social media, public information services, and emails. The information you gather helps you make decisions on combating future attacks or it can help you prevent attacks altogether. There are two main types of information gathered: the information a criminal requires to commit a crime and the information an attacker needs to take control of a target system. It’s important to know how a criminal may hack into your computer system so that you can test and prevent that method before it happens. For example, an attacker may perform a port scan to discover if a system is available and configured for telnet. By knowing this information, you can then conduct your own port scan to look for vulnerabilities before a cyber criminal does.

3. After gathering information about the different methods of attacks or current vulnerabilities within different systems the next step would be to hunt for evidence of the threat within your company.

4. After conducting searching and conducting tests within your own system, if you find any vulnerabilities you’ll want to immediately remediate them.

5. Lastly, and an equally important step as the rest is to record any findings. Write down what the threat was, how you found it, and what steps you took to prevent it.

Example of a Threat Hunt:

1. You gather cyber intelligence based on media reports, cyber crime groups, and breached data. Based on the information you determined that an account takeover is the biggest threat to your company.
2. You now need to list all of the accounts you have and begin reviewing

the account activity looking for indicators of potential compromise, such as login attempts. You find multiple failed login attempts from the same IP Address to one of your accounts.

3. Now, you check the account is secure by reviewing the accounts security measures such as updating the password or enabling 2FA (2-Factor Authentication) and insuring maximum security measures are in place.
4. After securing the account, you can use the data you gathered from the IP Address to reinforce other aspects of your cyber security such as blocking the IP Address from accessing your company's online assets.
5. Lastly, you make a record of this threat hunt because it showed indicators of a threat.

Making threat hunting a priority is imperative to your company's cybersecurity defense plan. Knowing what threats may arise and how your company is equipped to handle them could be the difference between whether your company succeeds or not. With adequate threat intelligence knowledge and constant monitoring you will be able to identify any threat that your network(s) or device(s) are susceptible to and be able to combat those threats before they are an issue. Also, keeping all software updated protects you from many known vulnerabilities.

Cybersecurity for Small Businesses

There’s no question that cybersecurity is a hot topic these days. With the massive Equifax breach making headlines in 2017, it’s more important than ever for small business owners to understand the basics of cybersecurity. While the big companies have the resources to invest in serious cybersecurity measures, small businesses often don’t have the same luxury. That’s why it’s important for small business owners to educate themselves on the basics of cybersecurity and take steps to protect their businesses.

Why Cybersecurity Matters for Small Businesses

Every business is at risk for cyber-attacks but small businesses are often the target of cyber attacks because they usually have weaker security than larger businesses. With cyber-attacks becoming more and more common, they can have a devastating impact on small businesses, costing them:

- Time,
- **$$$** Money,
- and Customers.

60% of small businesses that suffer a data breach go out of business within 6 months.

So, having poor cybersecurity not only risks all of your clients information, employees information, the business' financial assets and data, it's also taking away time and money that you would be investing into your business and risking the success of it.

Reasons to take cybersecurity seriously:

1. To protect your customers and employees privacy and information
2. To protect your business' data and assets
3. To ensure your business' long term succession

How to Protect Your Business

As a small business owner, it's not only imperative to understand the importance of cybersecurity but to also know the basics of how to protect your business from cyber threats. Steps that every small business owner can take to protect their business from cyber attacks, include:

1. Hiring a trusted cybersecurity firm
2. Educating yourself and your employees about cybersecurity.
3. Creating strong passwords using a password manager
4. Using two-factor authentication (2FA).
5. Keeping your software and systems up to date.
6. Backing up your data on a regular basis.

- **Hire a Cybersecurity Firm-** The best thing you can do for your company is to hire a trusted cybersecurity firm to monitor and test your company's computer networks. The field of cybersecurity is constantly changing with new techniques and software always being developed. As a small business owner you're not likely to have the time and expertise that is required to properly defend your business against cyber criminals.
- **Education-** You should educate your employees about cybersecurity threats and how they can protect themselves. This includes teaching them about phishing scams, social engineering attacks, and how to spot suspicious activity. Cyber attacks happen a multitude of ways including: social engineering, phishing emails and SMS messages, scam calls, vulnerabilities in third-party software, stolen/compromised credentials, and even insider threat attacks. By educating your employees, you can help them become your first line of defense against cyber threats.
- **Strong Passwords-** It is important to have a strong password policy in place for all of your employees. This means requiring employees to use strong passwords that are difficult to guess, and changing them on a regular basis. Additionally, you should have a process in place for handling employee password changes and resetting passwords if they are forgotten. Using a password manager, such as Bitwarden, is the best way to go. Password managers auto-generate unique passwords anywhere from 10-128 characters.
- **2-Factor Authentication (2FA)**– Setting 2FA on all able accounts is important so that any attempt to log-in to that account will require a second form of authentication. On the chance that someone figures out your password, they will not be able to get access to that account unless you approve the second form of authentication. Many people feel that setting up 2FA through SMS is protecting them, but in actuality it's

the most insecure form of 2FA. Ideally, using a 2FA application such as Authy or Bitwarden is the recommended way.

- **Updated Software and Systems-** Make sure that all of your software and systems are up to date with the latest security patches. This includes both your operating system and any applications that you use. Hackers are constantly finding new ways to exploit vulnerabilities, so it is important to keep your systems patched to protect against the latest threats.
- **Back-up your Data**– Your data should be backed up every 24 hours. This can me done manually or you can use automatic software to set a specific time for it to back up everyday. Having your data backed up protects you in case of system failure or file corruption.

Why Investing in Protection is Worth It
ext Here

As a small business owner, you are probably always looking for ways to cut costs. But when it comes to cybersecurity, skimping on protection can end up costing you a lot more in the long run.

Here are three reasons why investing in cybersecurity is worth it:

1. Data breaches are becoming more common – and more expensive.

- According to IBM’s 2022 data breach report, 83% of businesses will experience a data breach. The average cost of a data breach in the United States is $9.44 million. With more and more businesses falling victim to cyber-attacks, the chances of

your company being hit are increasing.

2. Cybersecurity insurance can help offset the costs of a breach.

- While no insurance policy can completely protect you from the financial fallout of a data breach, having cybersecurity insurance can help mitigate the costs. And, as the risks of cyberattacks continue to rise, so do the premiums for this type of coverage.

3. The costs of not investing in cybersecurity can be even higher.

- If your business is hit by a cyber-attack and you don’t have adequate protection in place, the costs can be devastating. Not only will you have to deal with the direct costs of the attack, such as data recovery and reputational damage, but you may also face legal action if your customers’ data is compromised.

So, while investing in cybersecurity may seem like an expense you can’t afford, the truth is that not investing can end up costing you even more.

How to Prepare for the Future of Cybersecurity

As the world becomes more and more digital, cybersecurity will become an increasingly important issue for businesses of all sizes. Small businesses are especially vulnerable to cyber attacks, which can have a devastating impact on their operations and bottom line.

Here’s what you need to know about the future of cybersecurity and how to prepare for it: Cybersecurity threats are

constantly evolving, so it’s important to stay up-to-date on the latest trends and developments. One of the biggest challenges businesses will face in the future is protecting themselves from sophisticated ransom-ware attacks. These attacks can encrypt your data and demand a ransom for the decryption key, which can be very costly. The best way to protect your business from ransomware and other cyber threats is to invest in a comprehensive cybersecurity solution. This should include robust monitoring software, firewalls, and user education. By taking these steps, you can help ensure that your business is prepared for whatever the future of cybersecurity holds.

As a small business owner it is important to be aware of the risks of cyber-attacks and take steps to protect your business. There are many resources available to help you understand and implement cybersecurity best practices. By being proactive and informed, you can help keep your business safe..

What is a Hacker and How Does Someone Become One?

When someone says “hacker” what’s the first thing that comes to mind? I’d be willing to bet that you thought of someone sitting behind a computer committing crimes through malicious activity, Did you know that the term “hacker” didn’t always have a negative connotation? Hackers are usually very skilled in programming and computer networking, and they have a good understanding of security systems and how to exploit them. The term “hacker” actually describes both the cyber-criminal and the “good guy” technological experts.To differentiate what

type of hacker one is, they are divided into different categories.

Types of Hackers

Hackers are categorized into 3 main types: white hat, black hat, and gray hat hackers. Although these different types of hackers go about it in very different ways, they all share one common goal: to find and exploit weaknesses in computer systems. The main difference between the 3 types of hackers is their motivation when they break into computer systems. Some are motivated by the challenge, others by the opportunity to make money, and still others by the desire to cause mischief or mayhem.

“White hat” hackers are ethical security hackers, or the “good guys.” Their motivation typically stems from their ethics and wanting to help company’s build stronger security systems. Many of them work as security consultants, they use their skills to find security vulnerabilities and help companies fix them before they can be exploited by the bad guys. They may also use their skills to expose security flaws in order to pressure companies to fix them.

“Black hat” hackers are the ones you typically think of when you hear the word “hacker.” They are the bad guys, the criminal hackers. They commit cybercrime usually for financial gain or to cause chaos through cyber espionage by exploiting security vulnerabilities and causing damage. They use their skills to steal sensitive information, commit identity theft, or launch attacks that disrupt websites or cripple computer systems.

Then, there are the “gray hat” hackers, who fall somewhere in between white hat and black hat hackers. Many of them believe they need to prove how unsafe the internet is for companies and individuals with the amount of data leakage.They use their skills, without consent, to find and exploit security vulnerabilities. Gray hat hackers don’t have malicious intent but they do often demand payment in exchange for full details of what they uncovered.

Sub-types of Hackers

Although most all hackers fall into one of the three categories listed above: white, black, or gray hat hackers, there are other sub-types of hackers: green hat, blue hat, and red hat.

“Green hat” hackers are new hackers, thus they’re inexperienced and lack technical skills. They may or may not have malicious intentions but they can be dangerous by accidentally causing damage whilst performing various cyber-attack techniques as they learn and develop new skills.

“Blue hat” hackers are people who are employed by a company or organization to look for any vulnerabilities or bugs within their security systems and/or soon-to-be released software. They look for vulnerabilities with a security system by conducting a penetration test, or pen test. A pen test is an authorized cyber-attack on a computer system conducted to evaluate the security of the system. Sometimes, a blue hat hacker references someone that is seeking revenge against someone; it may be a particular person, a former employer, or an entire country.

Lastly, there are “red hat” hackers, AKA vigilante hackers. Red hat hackers work to fight back against black hat hackers by taking matters into their own hands and infiltrating the black hat communities. Although noble, these hackers often use unethical or illegal methods to take down black hat hackers.

Which type of hacker are you?

Becoming a Hacker

How does one become a hacker? There’s no school teaching someone how to become a hacker. You can take courses teaching you about computer basics, the systems, and programming but hacking comes from learning to manipulate systems and programs into doing something they were not designed to do.

Most hackers:

- Are self-taught, and they are always looking for ways to improve their skills.
- Learn by trial and error; they are constantly experimenting with new techniques and tools.
- Are quick thinkers who can come up with innovative solutions to difficult problems.
- Are experts at finding and exploiting security vulnerabilities, and they have a deep understanding of how computer systems work.
- Are creative problem-solvers who are always looking for new challenges.

In conclusion, there are many different types of hackers out there. Some hack for good, some for bad, and some for personal gain. Whatever their motivation for hacking, some hackers can have a significant impact on our lives. They can cause financial damage, stress, and even jeopardize our safety. Be sure to stay informed and keep your computer security up-to-date to protect yourself from the dangers of the internet.