white paper

dash

cyberthreat guide

Six types of internet threats and how to help prevent them

dash

support you can rely on

introduction

Staying safe from cybercriminals is no easy task. Despite advances in cybersecurity technology, cybercriminals successfully pull off headline-worthy attacks all too often. In fact, it might even seem like cybercriminals are gaining the upper hand over many organizations. But why? First off, the number and types of cyberthreats have changed. For example, ransomware has become a major threat in many ways over the past few years. These attacks can be devastating and can even affect crucial services, like the damage to the United Kingdom’s National Health Service due to the WannaCry attack .

Second, the perpetrators have grown more coordinated and organized. While organizations must still worry about individual hackers or malicious insiders, they must now also contend with organized crime and even nation-state actors. According to the 2018 Verizon Data Breach Investigation report, 50% of data breaches were carried out by organized criminal groups . In short, the cybersecurity game has grown more complex—and the stakes are high.

ransomware

Ransomware is a type of malware that blocks access to or threatens to disclose a victim's data unless a ransom is paid. The truth is any organization is at risk of getting hit with a ransomware virus. In fact, ransomware can be so lucrative that several cybercriminals have implemented SaaS platforms to make ransomware attacks easier to execute against organizations—both large and small. The biggest dangers ransomware poses are the disruption, distraction, and downtime it can cause businesses.

Variations:

Some common and far-reaching variants include CryptoLocker, CryptoWall, Locky, WannaCry, NotPetya, and Teslacrypt.

what steps can i take?

Establish periodic system backup procedures, store backups securely, and test system recovery procedures to ensure they work. As long as your data is securely backed up and easily recoverable, you will reduce the likelihood of vulnerability to this type of digital extortion and blackmail.

It's also worth noting that when you back up your systems you should likely follow the 3-2-1 backup rule. This states that you should have three backup copies across at least two different media with at least one backup kept offsite. This can further reduce risk if local backups are corrupted or if the ransomware code attempts to delete local backups, as some ransomware strains attempt to do. And don't forget to periodically test your backups before they are needed. The last thing you want is to end up with a useless backup file in the middle of a data breach.

Additionally, make sure to monitor all critical systems, databases, and applications so you'll be able to detect suspicious access attempts and activities—before they get out of hand. You may want to add a SIEM tool to help you monitor for potential threats and act accordingly. Prioritize patching procedures, especially for security software, and perform regular vulnerability scanning against your public-facing assets.

what technology will help me detect, protect & respond?

- Patch management using Remote Managed services. This would have been especially applicable to the WannaCry crisis
- Managed Antivirus which is up to date
- Cloud / Offsite Backup
- Automated threat monitoring. Actively monitor for potential threats against your network using cyberthreat intelligence culled from multiple sources, network and host intrusion detection technology, and automated responses.

DDoS Attack

DDoS (Distributed Denial of Service) attacks work by overwhelming and disrupting an online service with traffic from multiple sources. DDoS attacks are nothing new. What is new is the way attackers are using the latest technology to amplify these types of attacks. By bouncing their DDoS attacks off a Memcached server (software used to accelerate web page load times), attackers can amplify the effect of an attack by up to 51,000 times . The largest DDoS attack on record was perpetuated against GitHub in 2018. In fact, reports show that the GitHub attack was twice as powerful as the DDoS attack that held the previous record from 2016 . While DDoS may not be the latest trick in the books, criminals still continue to use it—and innovate to make it more powerful.

Variations:

DDoS has been around for a long time. The latest innovations involve botnets and botnet armies that infiltrate systems around the world. A botnet of a few hosts is relatively harmless, but a botnet of thousands of machines could potentially be strong enough to bring down a victim’s operational environment. To produce faster resource exhaustion in the victim’s system, the attacker can slow the rate of response or hold open the TCP/IP connection by sending confusing, or non-RFC compliant, packets. This essentially tricks the server into thinking it will receive more data shortly. This is the equivalent of mimicking a bad cell phone connection.

what steps can i take?

A key to mitigating DDoS attacks is monitoring externally facing router and server performance. SNMP metrics can help you determine the load, connections, and error rates for any network interface—especially critical pieces of the infrastructure, such as firewalls. Tracking NetFlow from your' network devices can also potentially help you understand how much of their bandwidth is being used by legitimate "conversations," such as data moving between an internal system and an external provider, and how much is entirely inbound (a sign of potential DDoS activity). This could potentially help you locate threats or increases in conversations, protocols, or application traffic. Finally, inspecting inbound traffic by putting taps on, or mirroring, externally facing interfaces allows you to analyze inbound network traffic, and can likely give you a good indication of whether you are under attack.

In terms of stopping DDoS attacks, managed services providers (cloud providers, ISPs, DNS providers, etc.) will likely be the "first responders" on the front lines of these threats. By actively monitoring for this sort of attack and actively filtering, service providers can hopefully respond and mitigate, relying on each other to take steps toward orchestrating effective plans against these distributed and complex attack patterns.

what technology will help me detect, protect & respond?

Monitoring tools can be particularly helpful for these forms of attacks—particularly SNMP-based network monitoring tools (which are available from DASH). Use them to monitor for changes in performance that could hint at the possibility of an attack. Additionally, a managed RMM from DASH includes a web protection URL blacklisting feature designed to help prevent a system from making a call to a known CnC server. Finally, patching your systems can help prevent cybercriminals from gaining access via a system vulnerability

Brute Force Attacks

What are they?

Brute force attacks involve systematically looking for a correct network password. Successful attacks grant access to your IT infrastructure, whether network or server devices, with administrator-level privileges in many cases. At this stage, it’s unfortunately game over for the defenders. Brute force attacks—either from malware looking for its next host to infect or a malicious actor running a script—generally target a single service exposed to the internet, such as Remote Desktop, VNC, FTP, and SMTP services.

Depending on the robustness of security logging, these attacks may not be easy to detect. A high-volume brute force attack can exhibit similar patterns as a DDoS attack, only typically from just one or two IP addresses. Brute force attacks and their cousins, SQL injections, are threats to all services exposed to the internet. For example, if an attacker can guess a password for one of your content management systems, they can possibly gain unrestricted access to that account. If this site is hosted inside their company’s network, then complete network exploitation is possible

Variations

SQL injection attack: This occurs when someone attempts to “inject” SQL code directly into an application’s database without permission. This is a more sophisticated version of the brute force attack, as many different combinations of SQL injection need to be tried to gain access to the user ID and password table, which can frequently be unencrypted or poorly encrypted.

What steps can I take?

One good method designed to mitigate brute-force password cracking attacks is to limit the number of invalid logins (e.g., auto-lockout). In terms of protecting against SQL injection, remember there are two authentication modes used in SQL Server : Windows Authentication mode and mixed-mode, which enables both Windows Authentication and SQL Server authentication. The Windows Authentication mode is less vulnerable to brute force attacks, as the attacker is likely to run into a login lockout (the account-lockout-policy feature) after a finite number of attack attempts. In a production environment, consider making sure Windows Authentication mode is implemented and that you use the lockout-policy feature, as this is intended to make brute force attacks time- consuming and costly for the attacker. Additionally, it's important to remember you shouldn't use a domain administrator account as an SQL database connection account.

Also, review and consider strengthening your password policies, especially for databases, domain servers, and other critical systems and applications. Multifactor authentication can also help reduce the risk of these attacks. Additionally, make sure suspicious login activity is actively monitored, particularly for sensitive databases and production servers

What technology will help me detect, protect & respond?

Technologies that support and deliver multifactor authentication are intended to provide a robust level of protection against brute force attacks. Multifactor authentication relies on more than just what your users know (username and password). They combine this with another factor, such as what they have (e.g., your phone) or who they are (e.g., face ID). This approach is designed to make credentials more dynamic and less vulnerable to theft.

Additionally, consider choosing a threat monitoring tool to help augment strong authentication with nearly continuous and active monitoring and correlation of login activity. At DASH we can offer activity monitoring if needed

Phishing & Spear Phishing Attacks

What are they?

Phishing and spear phishing are forms of fraud where an attacker disguises themselves as a trusted entity to entice their victim to take an action (e.g., download a malicious attachment, go to a website, submit their credentials, etc.). This action is often the first step in a broader attack, where the attackers leverage stolen credentials from a “phish” to steal data, like medical records or intellectual property. The main difference between phishing and spear phishing is the scope of the intended audience. Phishing attacks are generally broad-based and widely distributed, whereas spear phishing is usually targeted at specific individuals or a group of individuals inside an organization.

variations

Cybercriminals often take their time in pulling up some of their biggest spear phishing traps to ensure they have a big payout. In fact, they will often create and store detailed profiles on their victims in databases on the dark web, collecting bread crumbs from social media platforms in their pursuit. While each of these campaigns may differ slightly in their initial approaches and tactics, these attackers typically aim for credential theft.

What steps can i take?

As with other forms of social engineering, educating your staff about how to engage online is a critical first step. When designing your security-awareness training programs, consider teaching your staff (especially executives) to practice good judgment and healthy skepticism when they engage on social media at work—both on the road and at home. Additionally, encourage them to think critically before opening email attachments or clicking links.

It may be worth testing security awareness programs on a regular basis by sending mock phishing emails to employees. You can then adjust their security awareness training components based on these assessments. There are tools you can use to test your preparedness for social engineering attacks.

What technology will help me detect, protect & respond?

At DASH we offer both on-premises training along with Online interactive training to bring your staff up to speed. Also available is Phishing Simulation to test how up to date your staff are when it comes to the bad guys

Drive-by Download

What is it?

A drive-by download refers to a website that automatically downloads malicious code onto a visitor’s machine. This can lead to devastating consequences, depending on what is actually downloaded to the victim’s machine. In October 2017, the city of Issaquah, Washington, was hit by a ransomware attack that took city services offline for four days . While the end result was a ransomware attack, the entry point was a drive-by download when an employee opened a PDF file on a website. In other words, a drive-by download took down a city for four days.

Cybercriminals commonly use exploit kits to distribute malware to users surfing the web. Such kits can include exploits for multiple vulnerabilities within a single malicious webpage. Subroutines in the code check out a website visitor’s target systems, web browsers, and browser plugins, such as Flash Player, Adobe Reader , Java , or Microsoft Silverlight for anything that isn’t fully patched. An attack is then launched to exploit that specific out-of-date software.

What steps can i take?

Web protection and filtering can potentially be a broader defense than antivirus in this case as it is designed to prevent employees from visiting known trouble hotspots. This can help reduce the chance of a malicious infection. This also means it can be used as a security awareness and education tool. At the other end of the scale, the reports that can be produced from a web protection and filtering tool can potentially be used to help explain poor internet performance, as well as potentially provide a solution to identify suspicious web traffic.

What technology will help me detect, protect & respond?

Patching—for everything from the operating system to antivirus definitions—is designed to be your main line of defense in this case. Consider investing in an intuitive patch management solution designed to quickly identify out-of-sync systems and address those software vulnerabilities in a way that gets the job done without impeding the end user's work.

Data Theft, Destruction, and Disclosure

What is it?

The December 2014 attack on Sony Pictures Entertainment set a new benchmark in the damage cybercriminals can inflict on an enterprise. In response to the damage this attack caused, including the release of highly compromising emails and data destruction, the FBI released a flash alert to warn other organizations of the danger. Elements of the Sony attack included massive intellectual property damage (through movie releases), data destruction, unauthorized disclosure of confidential information, denial of service (through credential theft), and reputational damage (leading to the termination of senior executives).

Variations

The Sony hack may be unique in the annals of cybercrime in terms of such a large collection of different security incidents happening rapidly over a short period of time. The motives seemed purely malicious. We included this attack, even though it's from several years ago, to demonstrate what can happen when an attacker is simply bent on destruction.

At no point did the attackers try to extort money from Sony—they only had digital mayhem in their plans. Given the state of cybersecurity and what feels like a continuous and unrelenting victory streak for the bad guys, a tremendous number of businesses would likely suffer the same damage from a similar cyberattack. Even if the malware used in this attack was not detectable by antivirus programs, Sony had a "passwords.xls" document that was neither encrypted nor password-protected that listed all passwords, including ones with administrative access.

What steps can I take?

Designing a simple, manageable network and establishing a continuous monitoring solution can potentially be easy wins. Often, data breaches occur when basic security measures simply weren't in place.

Security is about a great deal more, and combines the use of technology along with people and process elements. Consider starting with a security assessment, a plan to remediate critical items identified by the business, and then offer a solution to monitor the system for compliance. Simple measures often can be surprisingly helpful in reducing data breach risk.

WHAT TECHNOLOGY WILL HELP ME DETECT, PROTECT, AND RESPOND?

We should keep one thing in mind—all the hard work, diligence, and security technology will be ineffective if management at the company does not support and endorse a security program. If this is the case, you'll need to get really good at restoring data from backup.

The Sony attack is used in this paper to illustrate the worst possible scenario. The Sony attack demonstrates what can occur when the cybercriminals are simply bent on data destruction. The consequences of a massive data breach have evolved from the looting of personal private information and intellectual property theft to attempts to destroy or get paid for threatening to destroy a target. In any case, restoring data to its original state will likely need to be an end goal.

The Evolving Cyberthreat Landscape

Cybercriminals have multiple tools in their toolbox to attack businesses. And the truth is they will likely never stop innovating new ways to compromise systems or destroy data.

One thing that doesn’t change, however, is the importance of adopting a layered approach to security. The tools you use will depend on the types of threats you face. Most businesses will, at a minimum, need to keep up-to- date with basic cyberhygiene like patching, antivirus, web protection, and email security. However, many businesses should consider investing in more sophisticated security tools, like SIEM solutions and threat monitoring tools, which are designed to help against more complex cyberattacks.