June 2015

TechTidbit.com

brought to you by Tech Experts

Top Seven Network Attack Types So Far In 2015

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

There's no doubt that small businesses are under attack from hackers and cyber-criminals. Typically, small companies have less secure networks and looser security standards, making them easy targets.

The latest Threat Report from McAfee Labs details the types of attacks against small businesses. The chart shows the most common network attacks detected in Q1 2015.

Denial of service attacks – 37%

A denial of service (DOS) attack attempts to make a resource, such as a web server, unavailable to users. These attacks are very common, accounting for more than one-third of all network attacks reviewed in the report.

A common approach is to overload the resource with illegitimate requests for service. The resource cannot process the flood of requests and either slows or crashes.

Distributed denial of service (DDoS) attacks are popular today. This approach distributes the task to a number of computers.

Brute force – 25%

Some attacks look for a back way in, but a brute force attack tries to kick down the front door. It's a trial-and-error attempt to guess a system's password.

One in four network attacks is a brute-force attempt. Automated software is often used to guess hundreds or thousands of password combinations. There are many ways to defend against brute force attacks, but the simplest is to lock accounts after a number of failed login attempts.

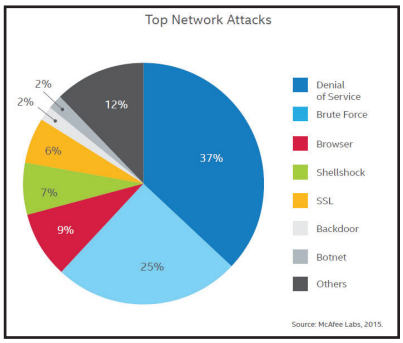
Browser attacks – 9%

Browser-based attacks target end users who are browsing the Internet. The attacks may encourage them to download malware disguised as a fake software update or application.

One of the best ways to avoid browser-based network attacks is to regularly update web browsers and browser-related services such as Java and Flash. This helps ensure newly discovered security vulnerabilities are patched before they can be exploited.

SSL attacks – 6%

SSL attacks aim to intercept data that is sent over an encrypted connection. A successful attack enables access to the unencrypted information. SSL attacks were more popular in late 2014, but they remain prominent today, accounting for 6% of all network attacks analyzed.



Shellshock attacks – 7%

"Shellshock" refers to vulnerabilities found in Bash, a common command-line shell for Linux and Unix systems.

Backdoor attacks – 2%

A backdoor is a type of attack that bypasses normal authentication to allow remote access at will. Backdoors can be present in software by design. They can also be enabled by other programs or created by altering an existing program. Backdoors are less common and often used as part of targeted attacks.

Botnet attacks – 2%

A botnet is a group of hijacked computers that are controlled remotely by one or more malicious actors. Millions of computers can be caught in a botnet's snare. The European Cybercrime Unit recently announced takedown of the Ramnit botnet, which infected more than 3.2 million Windows PCs.

The Basics Of HIPAA Compliance

Michael Menor is Vice President of Support Services for Tech Experts.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is federal legislation that created national standards to protect the privacy of patients' medical records (including electronic records) and other personal health information.

The legislation makes organizations and individuals who collect and manage personal healthcare data legally liable for its security, including health care providers, health plans, health clearinghouses and business associated with any of these. Consequences of negligence and misuse of private information can include civil and criminal penalties.

As a result of HIPAA, the Department of Health and Human Services created specific regulations for the handling of Protected Health Information (PHI), including electronic or digital forms (ePHI). HIPAA has two main sets of requirements related to privacy and security.

The HIPAA Privacy Rule governs the saving, accessing and sharing of health-related and other personal information, either oral or written.

This rule defines the guidelines safeguarding the confidentiality of PHI. Standards for identifying and authenticating people and organizations requesting PHI are outlined in this rule.

The HIPAA Security Rule more specifically outlines national security standards to protect health data created, received, maintained or transmitted electronically.

This rule primarily focuses on the technological measures used to enforce policies keeping ePHI out of the wrong hands. Failing to comply with these rules can result in penalties for not only organizations, but for the responsible individuals.

Any entity that deals with protected health information must make sure that all the required measures are established and continuously observed — physical (actual data center server access), network, and process security (audits, policies and staff training).

While the legislation is clear on the privacy, security, and accessibility requirements for organizations, over 91,000 violations were recorded between April 2003 and January 2013. These resulted in 22,000 enforcement actions (which included settlements and fines) with 521 referred to the US Department of Justice for criminal investigation.

HIPAA Compliant Best Practices

1. Review and evolve your policies and procedures. HIPAA is not a "set and forget" proposition; compliance must be a living, changing process that is regularly audited for effectiveness and legality. A lot has changed since 1996 and organizations' policies must reflect those changes.

2. Accessibility rights are as important as rights to privacy. HIPAA gives patients certain control over their healthcare information, including the right to access it on demand and the right to revoke authorization to store their data. Organizations must act quickly when patients ask for their PHI.

3. If you store your data with a third party hosting provider, make sure that they are HIPAA compliant. The Security Rule hands down many stringent administrative, physical and technical requirements for such providers. Make sure that a full-scale risk assessment of the provider is performed on a regular basis and that a process is in place for monitoring compliance.

Apply common sense to your technology platforms. Shut down computer programs and servers containing patient information when not in use, and don't share passwords among staff members.

The US Department of Health and Human Services has found that storing patients' information in a HIPAA compliant cloud server can be safer than using a localized server or paper documents, so consider this option for increased security.

A HIPAA violation can be as small as a health care worker discussing a patient's private health information in the elevator or as large as a $1.2 million fine for not erasing PHI from photocopier hard drives before returning them to the leasing agent.

More than ever, common sense and sound corporate governance must be applied to the technologies and processes that manage confidential data. Protecting that data will protect clients and the organization as well.

Documenting Business Processes

Scott Blake is a Senior Network Engineer with Tech Experts.

Documentation is quite possibly the most important aspect of a business, but it can also be workers' least favorite task to do. The average person doesn't want to spend time writing down how they do something — they just want to do it and move on.

Can you guess the biggest reason for documenting your business processes? It may come as a surprise, but it's also the most fluid part of your business: your employees.

Employees come and employees go and some just take vacations. It's what they do in between that's important. Every employee is responsible for some part of your daily business.

Whether an employee quits or just needs time off, having documentation that lists the software used with usernames and passwords, step-by-step instructions on how to use the business software, client and vendor contact information, and credit card information makes their absences that much easier to deal with.

Well-documented processes will cut down on the time it takes to train a new employee. Give the related information to the new employee and let them use it as a guide for their daily activities. This will allow your other employees to spend more time on their tasks and assignments instead of spending the majority of their time answering routine questions that a documented process could answer.

Order-of-operation questions and disputes can be minimized as well. If there ever comes a time when your employees are unsure of the next step or there is a dispute between departments on how to proceed, they will only need to look over the documented processes in question to resolve the issue.

Having documentation that shows in detail how long it takes to produce a product will also help your sales force deliver your product to your customers.

It allows your sales and marketing departments to understand the timelines of production.

This knowledge will let them know when a product order can be delivered and if the amount can be fulfilled in the timeline requested by the customer. There will be no more over or under promising of delivery dates to customers.

Put trust in the documents, not the person. No one person should be trusted with remembering processes without documenting them. What if this employee quits or becomes ill and is unable to return to work? For example: You have an employee that works in your IT department. This employee's job is to monitor and resolve any network related issues. While doing his daily tasks, he discovers it's time to change the passwords on the business networking equipment such as the router, managed switches and domain admin password.

While the employee doesn't think twice about it and may have mentioned it to his manager, there was nothing ever documented. Now, four months later, the employee falls very ill and is unable to return to work. What do you do?

The best way to document your business processes is to document them in such a way that all contributing employees have access.

You could use online tools such as Google Docs or Microsoft SharePoint. This way, whenever a process is changed, amended, or removed, the documentation is instant and available for all to see.

After a while, you will have an impressive collection of documented procedures. Having documented information available for employees to read can also start the flow of constructive questions and comments why things are done a certain way and how they can be improved.

If you have questions or you're looking for suggestions on documenting your processes, call Tech Experts at (734) 457-5000.

Create new service requests, check ticket status and review invoices in our client portal: http://www.TechSupportRequest.com

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Three Sure-Tell Signs Your Hard Drive Is Failing

Under ideal conditions, the average stationary hard drive lasts five to ten years. With the growing use of external drives and laptops that are toted around frequently and exposed to damaging elements, that life span shrinks to between three and five years.

Consequently, it is important to watch for indications that your hard drive is failing, so you can back up all of your valued files and data. Here are three signs that it's time to act:

Slowed Operation and Freezes

You should immediately back up the contents of your hard drive when you notice that freezes and display of the blue screen become the norm.

It is even more imperative to do so, if these problems continue in Safe Mode or after a fresh installation of your operating system because that's an indication that hard drive failure is imminent.

Corrupted Data

When it becomes problematic to save or open your computer's files and you start getting error messages about corrupted data, you should know that your hard drive is failing.

As a hard drive's functionality gradually wanes, this is a common problem, so act fast to ensure your business and personal data stays intact and safe.

Presence of Bad Sectors

If your hard drive has bad sectors, or areas incapable of maintaining data integrity, you may not immediately notice the problem.

The presence of such sectors is a grave problem and tells that your hard drive is in its final strides.

To check your hard drive for bad sectors, run a disk check with the options to automatically fix the problem and attempt recovery of files.

Coming Of "Edge:" Microsoft's New Browser

Up until now, Internet Explorer's successor has been secretly referred to as Project Spartan during Microsoft's development stage. At the Microsoft Build 2015 Developer Conference, the project name was finally announced as the company's newest browser: Edge.

The name was already familiar to those in the know because Project Spartan's page-rendering engine was known as Edge, but now the name has been elevated to describe the product as a whole.

For those who have had difficulties with Internet Explorer, this new browser is long overdue, but Edge should turn their frowns into smiles because it is much faster and more compatible with modern web standards.

Edge joins its competitors, like Firefox and Chrome, in the use of extensions and actually uses the same JavaScript and HTML standard code.

This means that Microsoft's new browser can easily adopt its competitor's extensions. In fact, Joe Belfiore, Microsoft's VP of Operating Systems Group at Microsoft, demoed a couple of extensions at the conference. However, you won't see the extensions feature in Windows 10 until later this year.

Cortana, Windows 10's Siri-like virtual voice assistant, makes an appearance in Edge as well. When needed, Cortana shows up in a blue circle in the browser's toolbar to relay pertinent information related to the landing page, such as directions to a local business or contact information.

Edge users can also summon Cortana for assistance and extra info by right-clicking on text selections to find out more.

Another Edge feature is the new-tab page, a remnant from Internet Explorer with a few tweaks. When Edge users open a new tab, the page displays thumbnail icons for the most frequently visited sites. It also allows users to reopen closed tabs and makes many suggestions for apps and videos and facilitates access to weather or latest sports scores.

Edge also provides the option to view pages in a reading mode free of distractions such as images and advertisements. Users can even make annotations, such as highlights and notes, on webpages for sharing or storing as an image. Microsoft's new browser also comes with coding support and will function the same across all platforms. Until Edge is formally released, users can test it on non-critical PCs by downloading Windows 10 and joining the Windows Insider Program.