ANP ADVANCED NETWORK PRODUCTS

TOP TEN MOST COMMON CYBER SECURITY THREATS

AND HOW TO START PROTECTING YOUR BUSINESS NOW

Introduction

Cybercrime is at an all-time high, and hackers are now setting their sights on small and medium businesses as "low hanging fruit" because they don't have the proper technologies in place to combat these sophisticated attacks.

Don't be the next victim!

This report reveals the most common ways that hackers are gaining unauthorized access into businesses today and how you can improve the security of your small or medium business.

Is your network truly secured against the most devious cybercriminals? What do you need to do (at a minimum) to protect yourself now? This report will help you determine if you're doing enough.

#1: WEAK PASSWORDS

A weak password policy increases the probability of an attacker having success using brute force and dictionary attacks against user accounts. An attacker who can determine user passwords can take over a user's account and potentially access sensitive data in the application.

It is therefore important that this password be of sufficient complexity and impractical for an adversary to guess. The specific requirements around how complex a password needs to be depends on the type of system being protected. Selecting the correct password requirements and enforcing them through implementation are critical to the overall success of the authentication mechanism.

Following established advice on password length and complexity is a good first step. However, this does not mitigate users' tendencies to pick passwords based on common words, with additional character substitutions.

For example, a user may choose a password such as **Password1**!, which may satisfy length and complexity requirements (at least 10 characters long and a mixture of upper- and lower-case letters, digits and special characters). Unfortunately, this is a commonly used password, and can be found in most dictionaries compiled for password cracking.

"73% of users duplicate their passwords in both their personal and work accounts. This is why compromised passwords are responsible for 81% of hacking-related breaches."

Verizon Data Breach Investigations Report

Recommendations:

• Use "pass phrases" with two or more words, which will greatly increase the search space required to succeed in a brute force attack. These may also be easier to remember than complex substitutions on a single word.

• Don't rely solely on lockout thresholds to protect against users' choice of weak passwords; hashed credentials can be leaked from databases and the internal corporate network.

• There's more to password strength than using difficult to remember character substitutions and complex characters – encourage users to use longer combinations of words which may be easier to remember.

• Consider auditing your passwords periodically to identify accounts with weak passwords, especially privileged or administrative ones.

• Don't forget to change business-related service passwords regularly.

#2: MALWARE

Malware is the shortened name for malicious software and is an umbrella term used to categorize a variety of forms of hostile or intrusive software. Everyone is vulnerable to malware. Attackers will target any organization of any size, including:

- Small to medium sized businesses
- Large corporations
- Healthcare providers
- School districts
- Government agencies
- Law enforcement agencies

Here are some of the most common types of malware and how to identify them:

1. Trojans
A Trojan (or Trojan Horse) disguises itself as legitimate software with the purpose of tricking you into executing malicious software on your computer.

2. Spyware
Spyware invades your computer and attempts to steal your personal information such as credit card or banking information, web browsing data, and passwords to various accounts.

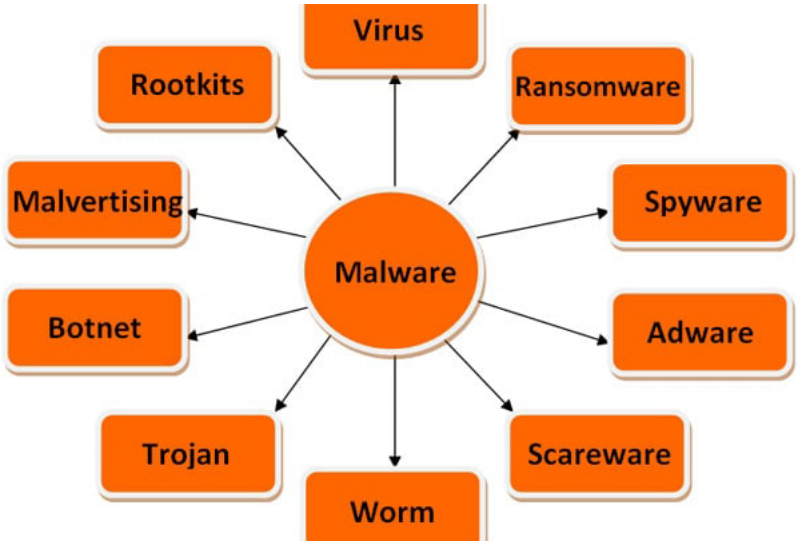
3. Rootkits
Rootkits enable unauthorized users to gain access to your computer without being detected.

4. Adware
Adware is unwanted software that displays advertisements on your screen. Adware collects personal information from you to serve you with more personalized ads.

5. Ransomware
Ransomware is designed to encrypt your files and block access to them until a ransom is paid.

6. Worms
A worm replicates itself by infecting other computers that are on the same network. They're designed to consume bandwidth and interrupt networks.

7. Keyloggers
Keyloggers keep track of your keystrokes on your keyboard and record them on a log. This information is used to gain unauthorized access to your accounts.



#3: RANSOMWARE

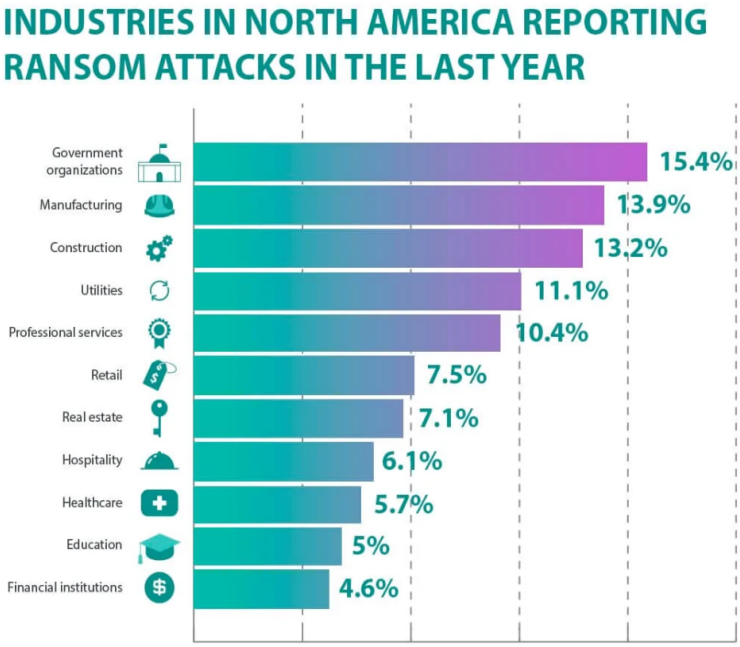
Although Ransomware is in fact a type of malware, it is one of the most disruptive and prolific security threats today, and it's shown that it can debilitate any business therefore should be represented as its own type of attack. While initially targeting individuals, later ransomware attacks have been tailored toward larger groups like businesses with the intent of yielding bigger payouts.

Popular ransomware variations lock organizations and end users out of their computers, data, and networks. This halts critical computer systems until the victim pays a ransom. Although ransomware typically targets businesses via phishing attacks, hackers often use methods like worms to infect all computers that connect to a network.

Ransomware is a type of malware, a software program intended to damage computer files. It quietly invades your computer, encrypting as many files as it can locate on your local and network drives. The encryption is done by using a complex mathematical algorithm. When the encryption is complete, your files become unreadable unless you have the key to unlock them.

The only one with the key is the cybercriminal who demands you pay a ransom in order to regain access to your files. Your data has been kidnapped. A simple virus scan cannot undo the encryption. Your data is being held hostage by the cybercriminal.

In many cases, there is a time limit for payment. A count-down clock may even appear on your screen telling you that you must pay the ransom within a certain period of time or forever lose access to the files.



Recommendations:

There are several things you should do to prevent a ransomware attack but here are 2 important recommendations to start.

1. Educate your end users! Teach employees to follow safe computing practices, how to identify a phishing email and to avoid clicking on suspicious links.

2. Have a good backup solution in place so you can quickly restore it without needing to pay the ransom.

#4: UNPATCHED VULNERABILITIES

Cybercriminals exploiting unpatched system vulnerabilities continue to be one of the top reasons businesses suffer unauthorized intrusions. With the increasing number of interdependent online infrastructures and devices, proper patch management and procedures is more critical than ever.

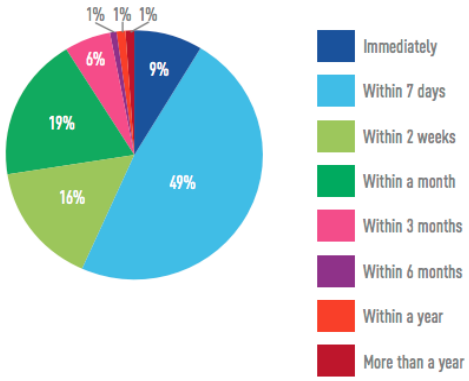
And while the task of patching systems can be time consuming, past incidents have shown that failing to patch systems with the latest security updates can prove to be extremely costly.

In fact, one in three breaches are caused by unpatched vulnerabilities. Each year there are more than 11,000 vulnerabilities reported to the Common Vulnerabilities and Exploits (CVE) database, many which are still unpatched.

The WannaCry ransomware attack which targeted computers running Microsoft Windows OS, is just one painful reminder of how an unpatched vulnerability can spread globally with disastrous results in a very short period of time.

More recently, it has been noted that Cybercriminals are launching Remote Desktop Protocol (RDP) attacks by using BlueKeep, a "wormable" vulnerability that self-replicates malware to spread across the Internet rapidly. A compromised RDP server can then quickly invade networks consisting of millions of Internet-connected RDP servers.

How long does it take to deploy a security patch?



Recommendations:

1. Automate updates!

2. Backup your systems. It's the cheapest and easiest "insurance" you can buy for your critical systems.

3. Avoid downloading or using free software.

4. Use a recent and high-quality antivirus software and make sure those are set to automatically update.

5. Use real-time data feeds which enable you to block traffic to known malicious sites and are designed to provide continuous updates.

6. Advise teams across your entire organization if and when there is any sort of security warning with a reminder to be extra vigilant.

7. Don't forget, hardware needs patching too!

#5: ZERO DAY ATTACKS

A zero-day (or 0-day) vulnerability is a software vulnerability that is discovered by attackers before the vendor has become aware of it. At that point, no patch exists, so attackers can easily exploit the vulnerability knowing that no defenses are in place. This makes zero-day vulnerabilities a severe security threat.

Once attackers identify a zero day vulnerability, they need a delivery mechanism to reach the vulnerable system. In many cases the delivery mechanism is a socially engineered email – an email or other message that is supposedly from a known or legitimate correspondent, but is actually from an attacker. The message tries to convince a user to perform an action like opening a file or visiting a malicious website, unwittingly activating the exploit.

A zero-day attack typically proceeds as follows:

1. Looking for vulnerabilities – attackers search through code or experiment with popular applications, looking for vulnerabilities. They may also buy vulnerabilities on the black market (see more details about zero-day markets below).
2. Exploit code created – attackers create a malware program or other technical means to exploit the vulnerability.
3. Looking for systems affected by the vulnerability – attackers can use bots, automated scanners and other methods to identify systems that suffer from the vulnerability.
4. Planning the attack – in a targeted attack on a specific organization, attackers may carry out detailed reconnaissance to identify the best way to penetrate the vulnerable system. In a non-targeted attack, attackers will typically use bots or massive phishing campaigns to try to penetrate as many vulnerable systems as possible.
5. Infiltration – an attacker gets through the perimeter defenses of an organization or personal device.
6. Zero-day exploit launched – attackers are now able to execute code remotely on the compromised machine.

#6: BACKDOOR PROGRAMS

A backdoor cyberattack is any type of cyberattack — the deployment of malware, keyloggers, viruses, phishing, etc. — that involves bypassing a computer's or network's conventional authentication system without being detected.

During a backdoor cyberattack for example, a hacker will bypass the login portal, thus gaining access to the computer's files without proper authentication.

The way in which a backdoor cyberattack works varies depending on the specific type of attack. Some backdoor cyberattacks involve exploiting a vulnerability in a computer or network. If a computer is running an outdated operating system, for example, a hacker could potentially bypass the computer's authentication system to gain administrator access.

Some backdoor cyberattacks work in conjunction with malware, meaning, hackers can create a backdoor on a computer or network using malware.

#7: SHADOW IT

When new applications, devices, software make their way onto your network without consent from your IT department that is Shadow IT.

The truth of the matter is, we as humans tend to gravitate towards the simplest solution. We have grown comfortable with searching and downloading apps online to help us do our job more effectively. And with the abrupt move to working from home in recent months, many users are finding workaround to easily access their data and collaborate with colleagues on files. As a result, businesses' applications have moved from behind the safety of the company firewall to public Software-as-a-Service (SaaS) solutions for everything from accounting, to marketing, to human resources.

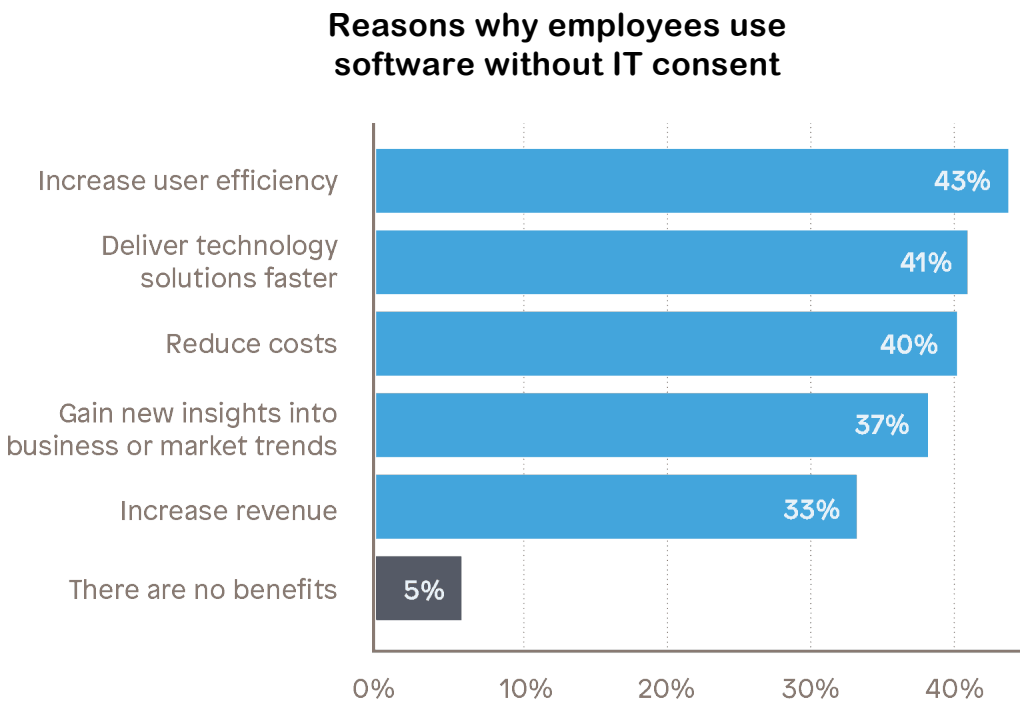
This puts IT in the uncomfortable position of saying no to employees that request access to desired cloud apps to be more productive. However, for every app that's blocked, there's evidence employees are finding other, lesser-known, and potentially riskier services to use in its place.

• Find out why your users are circumventing the IT department with Shadow IT applications and devices.

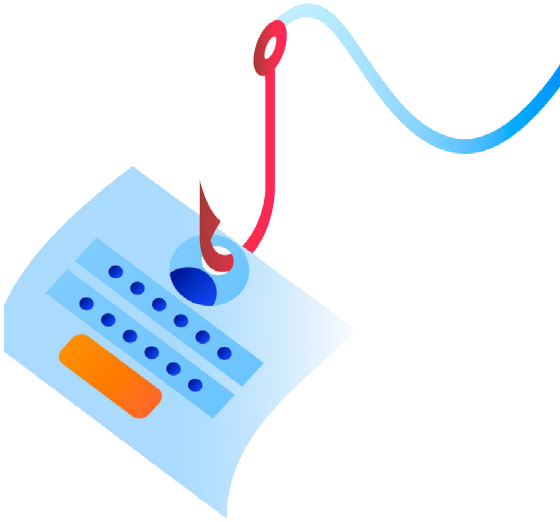
• Make IT more accessible. Emails containing new policies are often overlooked. Take the time to explain why these policies are in place and share implications of Shadow IT.

• Educate colleagues on policies. It's important to ensure they understand these policies and why they're set.

• Stay up to date on modern technology solutions and make them accessible when a strong use case is presented.



#8: PHISHING ATTACKS



A phishing e-mail is a bogus e-mail that is carefully designed to look like a legitimate request in an effort to get you to willingly give up your login information to a particular web site or to click and download a virus. The email is usually sent out blindly to a list of email addresses purchased off of the dark web, in an effort to get a bite, hence the name.

Often these e-mails look 100% legitimate and show up in the form of a PDF (scanned document) or a UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, etc.

90% of the malware businesses encounter is delivered via email.

SPEAR PHISHING: Spear phishing is an email aimed at a particular individual or organization. These hacks are not executed by random, rather they are specifically selecting their victim and tailoring their message to attempt to gain access to your system.

Often, spear phishing emails appear to originate from an individual within the recipient's own organization or someone the target knows personally. Cybercriminals also carry out these attacks with the aim of reselling confidential data to private companies and governments. These attackers employ social engineering and individually-designed approaches to effectively personalize websites and messages.

WHALING: This is a term used to describe phishing attacks on high-profile business executives, such as a CEO or even the head of the accounting department. Typically they will use spoofed emails to very closely mimic a legititmate email request, or wire transfer.

SOCIAL ENGINEERING: Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data.

For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password. They could also use social media to fill in gaps on your profile, or come up with a much more targeted plan of attack such by referencing information about you that only your friends, family and workplace may know.

#9: UNMANAGED IOT DEVICES

Technology has made our lives better. However, the growing reality of the IoT also means recognizing its possible consequences. In an enterprise setting, for example, the IoT is often seen in the office automation (OA) and operational technology (OT) areas. This translates to multiple IoT and IIoT devices deployed within an organization. Such a setup increases the possibility of threats in spaces that had never posed cybersecurity risks before.

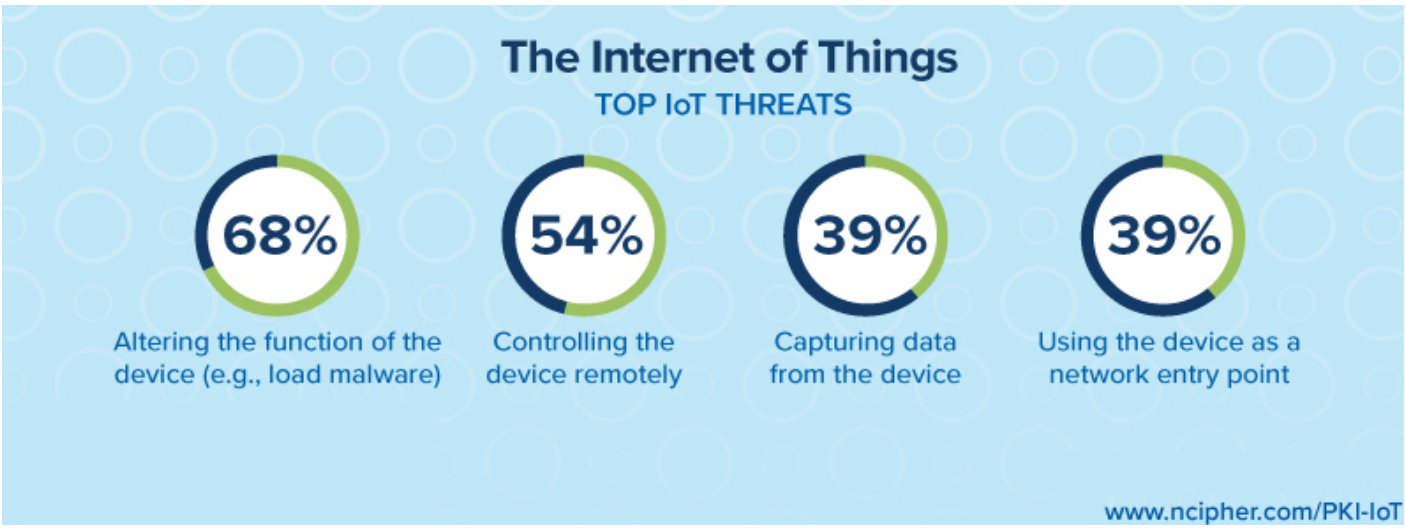
Most companies and consumers have taken advantage of this amazing sourced of information to: conduct business, search and gather information, communicate with associates, friends, and family through email and social media, access retail and business-to-business (B2B) sites to make purchases and more.

IoT takes the internet to the next level. With this technology, connectivity enables connected devices to communicate with each other directly – removing the need for human interaction. Some common examples include:

- Home security systems and doorbells that communicate directly with devices such as smartphones
- Industrial automation with sensors in manufacturing environments that can be managed remotely with connected devices
- Marketing strategies that utilize IoT kiosks in retail locations to notify shoppers via smartphone alerts about sales and other offers in their proximity.

Usually, attackers who target IoT devices don't want to cause you a problem. They use your device as a "soldier" to battle – along with 20,000 other thermometers – against an Internet website, e-mail server or another Internet target.

That much traffic could be enough to make a website quit working, or stop your e-mail server from delivering e-mail to you. You should adopt a very strict offensive posture against these types of threats in your business and life. If there is a problem, you should be comfortable with the approach of "kill first, ask questions later."



#10: SUPER ADMIN ACCESS

Today's IT managers face the continued challenge of finding that perfect middle ground between a guaranteed secure network environment and one that is conducive to user productivity and innovation. Such is the case when allotting admin rights to users.

The importance of implementing privileged access management (PAM) is undeniable. A user with privileged access holds the keys to the kingdom, access to the highly valuable and confidential information that is often targeted by cybercriminals and malicious insiders.

Recommendations:

1. Establish consistent Access control processes

2. Audit and track user behavior

3. Take Control of your Privledged Access Management

Data protection is a central component of cyber-security policies and solutions. Typically, it discusses threats to your company's data integrity or privacy. According to a recent report, many employees can access too much data. This makes internal threats as dangerous as external ones.

The report states that 48% of employees have access to more information than they need to do their jobs. Alarmingly, 12% of companies give all employees access to crucial company data. And if one person becomes upset with the company, this could spell disaster. To address this potential, preventable risk, it's recommended to develop a strong data classification system for your organization.

74% Of Data Breaches Start With Privileged Credential Abuse

Conclusion

ANP has been helping hundreds of businesses across Philadelphia, New Jersey and Delaware to keep their network and data safe for over 36 years. In this time, we've learned that no one security tool or program can keep the bad guys out. Cybersecurity is constantly evolving and requires a multi-layered approach to prevent a data breach.

We've tested all of the industry leading security tools and have compiled a security bundle that allows small and medium businesses to leverage enterprise technology at an affordable price point. To learn more about our cyber security services visit us at **https://www.anp.net/managed-security-services**

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

The first step is a no obligation cybersecurity risk assessment:
https://www.anp.net/cybersecurity-assessment

CYBER SECURITY ASSESSMENT:

Is your business at risk for a cyber attack?

CLICK HERE to find out now:
https://www.anp.net/cybersecurity-assessment