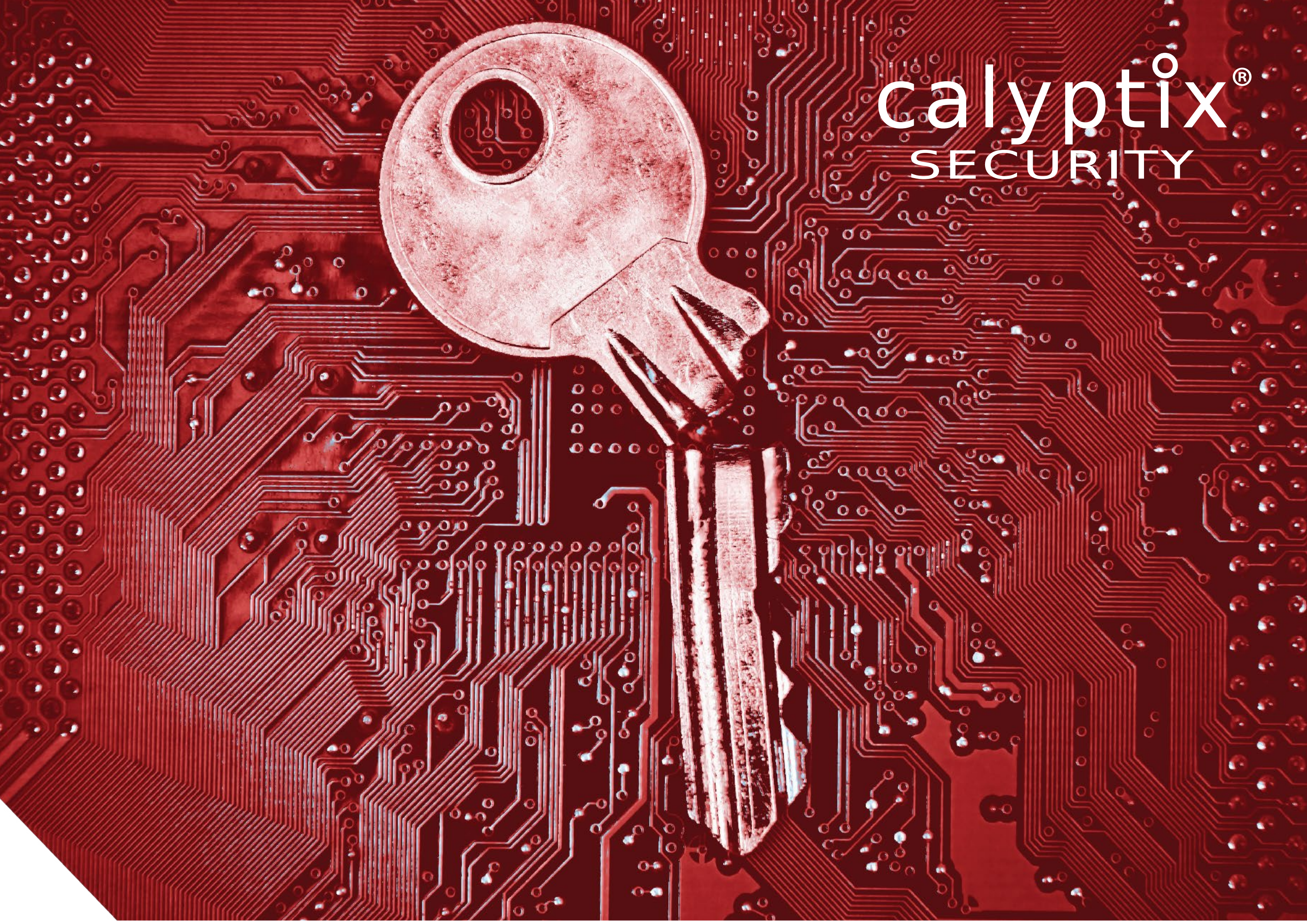


Top Security Threats | 2017

What's Ahead and How to Prepare

Contents

intro.

The news is full of blockbuster data breaches. Company Y is attacked and loses *one zillion* customer records. Political Party P is hacked and has its emails leaked for the world to see.

Small companies hear the news and breathe of sign of relief, “Wow, we’re lucky this happens only to the *big* guys!”

But these attacks are only part of the story.

The rest of the story – and some would say the bigger story – is the growing number of cyber attacks against small businesses. Every day, new ransomware attacks, denial-of-service attacks, phishing attacks and others, threaten the existence of thousands of businesses across North America.

The hazards are often ignored by the press but they are critical to small businesses nonetheless. If your company is connected to the internet in 2017, then you must know and prepare for these threats.

This report covers the top five cyber security threats for small businesses in 2017: Ransomware, Malicious Email, the Internet of Things, Vulnerabilities, and Bad Habits.

Ransomware

Ransomware continues to harm businesses of all sizes. The number of attacks spiked in 2015 and remains high, fueled in part by the millions of dollars the scams earn for attackers. The trend shows no signs of ending soon.

Background

Ransomware is a type of malware that blocks access to a victim's assets and demands money to restore that access. Almost all ransomware today is "crypto-ransomware," which blocks access to a victim's files through encryption.

Once a victim is infected, the ransomware scans the available local and network systems for important files, such as those associated with Microsoft Office, images, and backups. It then encrypts the files and alerts the user to the infection. The alert includes a ransom demand and a deadline for payment.

If victims do not pay in time, the ransomware destroys the decryption key and the victim's files are rendered useless. If the payment is made in time, victims usually receive a decryption key to unlock their files (though not always).

Attacks Continue to Rise

Ransomware has many different strains and they continue to multiply. A few are Locky, CryptoWall, CryptXXX, CTB-Locker, and the list goes on and on.

The number of ransomware families spiked in 2015 and continued to grow rapidly in 2016, according to Trend Micro (see chart). Growth from January to September 2016 in ransomware families reached 400%.

Though many ransomware strains are inactive, many more have replaced them to continue making money for thieves.

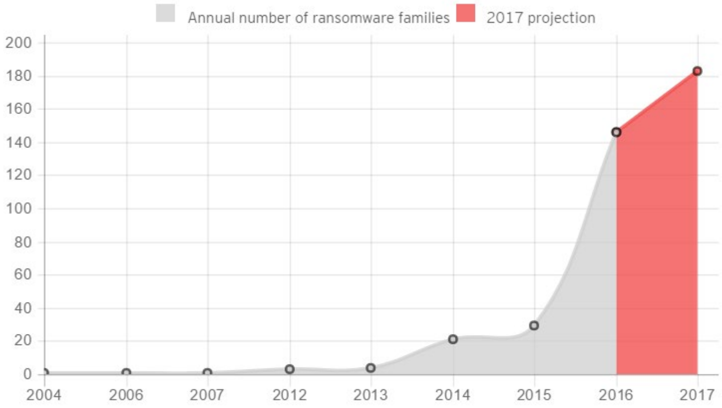


Figure 1: Annual number of ransomware families, including 2017 projection

Why Ransomware is Spreading

As a means of cyber attack, ransomware has been around for over a decade. Why did it explode in use a couple years ago, and what's keeping it around?

Easy to access

A few years ago, only experts could launch a sophisticated crypto-ransomware attack. Today, ransomware-as-a-service makes it easy for laymen to rent the architecture needed to deploy attacks and collect money. Open source versions of ransomware were also released last year, helping to fuel more growth in the crime.

Fast money

Thieves have discovered something about ransomware: it works. With modest technical skills and relatively small investment, hackers and wannabes can quickly generate thousands of dollars in extorted income.

CryptoWall 3.0 alone is estimated to have earned $325 million. The FBI estimates $209 million was paid in all ransomware schemes in just the first three months of 2016. [6] [7]

Fighting the rise

Not all ransomware trends are bad. Some experts suggest the rapid growth seen since 2015 is not sustainable and will slow in 2017. The ongoing efforts of law enforcement and the security industry to eliminate ransomware strains and shut down their architecture is helping to slow the spread. Organizations such as ***No More Ransom!*** are creating free tools to help victims unlock files that were encrypted by certain strains of the malware. [8]

Attacks with Narrow Targets

The average ransom demanded from victims increased in 2016, and this is driven in part by a trend of launching targeted attacks against vulnerable organizations with the means to pay quickly.

By carefully selecting targets, attackers can increase their chances of success and demand higher ransoms. For example, organizations with a high dependence on sensitive data, strained IT staff, and deep pockets, can be more lucrative targets.

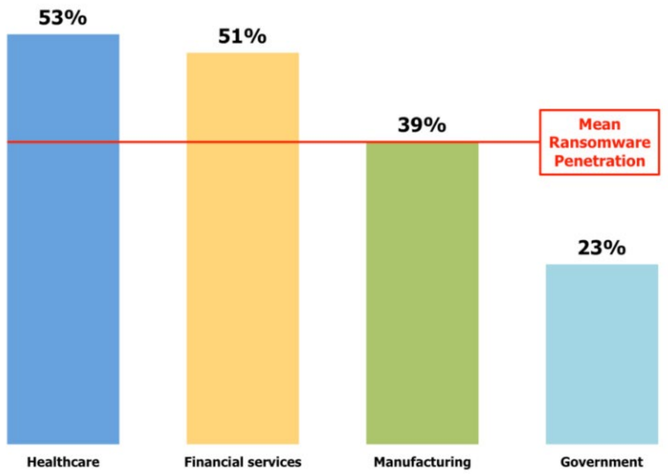
Many healthcare organizations fit this profile, especially hospitals. Their growing reliance on electronic health records, which are critical to patient care, combined with a reputation for poor cyber security and large amounts of revenue, make them fat chickens to the wolves of cybercrime. And the wolves are on the hunt.

One example is the attack on Hollywood Presbyterian Medical Center. After two weeks of haggling with attackers, the hospital ultimately paid $17,000 in ransom to unlock its records and restore its systems. Experts suggest the attack was performed with Locky ransomware, which spreads via phishing emails. [9]

While some reports put the healthcare industry's share in overall ransomware attacks as high as 88%, others suggest the financial services industry is also seeing more attacks than average. [10]

The chart below from an Osterman Research survey shows more than half of all respondents in the healthcare and financial services industries reported a successful ransomware attack in the last 12 months. [11]

Figure 8
Ransomware Attacks That Have Occurred During the Previous 12 Months
Includes data from the four geographies surveyed



More Trouble Ahead

Ransomware will continue to fester in 2017, and experts say attackers are likely to begin experimenting with new tactics. Below are a few anticipated trends.

New victims targeted

Attacks on hospitals were unrelenting in 2016 and are likely to continue. However, attackers may experience diminishing returns by focusing on these targets too long. Other healthcare organizations, such as small doctor's offices or insurance providers, may be next. Some have even suggested the targeting of medical devices, such as pacemakers, that can connect to the internet.

New hardware targeted

A change in the platforms targeted may also be on the horizon. Potential targets suggested by experts include mobile devices, point-of-sale systems, and ATMs.

New revenue streams

Attackers may also adapt ransomware to steal data as well as encrypt it. This way, they can double their money – not only by ransoming the data, but also by selling it on the black market.

More attackers

As ransomware continues to grow and spread, it is likely that this weapon will reach the hands of criminals who have weaker discipline and skills. This could result in an increase in ransomware attacks that fail to decrypt files once a payment is made, and also could diversify the types of victims targeted.

Protect your business

The time to prepare for a ransomware attack is not when multiple workstations in the office are flashing demands for Bitcoin payments. Steps must be taken beforehand to prevent the infection and minimize its impact.

Watch the main entry points

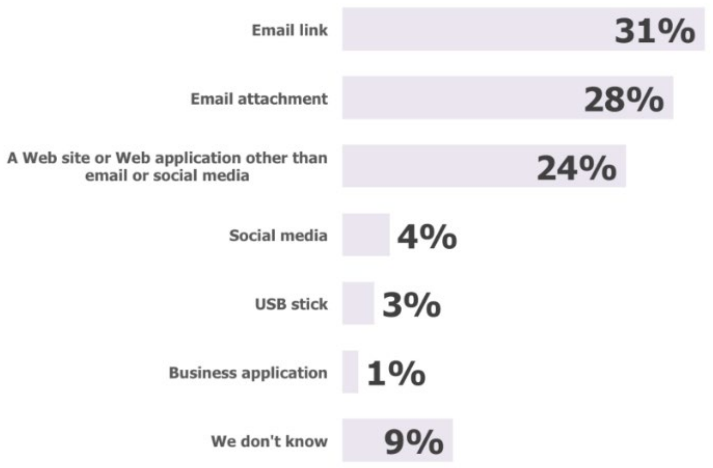
Email is the favorite channel for ransomware to enter the organization. As this chart shows below, it accounts for more than half of all infections reviewed for on Osterman Research report published in August 2016. The only other significant channels are websites and web applications. [12]

Clearly, all organizations must use email filtering and web filtering to block malicious content before it reaches users.

Filter outbound traffic

Also consider using outbound traffic filtering (a.k.a. egress filtering) with a "default-deny" policy. This will block all outbound connections except for those explicitly allowed through rules set by the administrator. This can prevent ransomware from communicating with command-and-control infrastructure and prevent some infections from fully taking hold.

Figure 12
Applications by Which Ransomware Entered the Organization



Source: Osterman Research, Inc.

Group policies for Windows

Group Policies are available that can block many variants of ransomware from installing in their favorite directories in Windows. The policies and more information are available in the Ransomware Prevention Kit from Third Tier, a Calyptix Partner. Check the resources at the end of this report for a link to Third Tier's kit.

Back up all files

The number of small businesses that operate without backups is staggering. If such an organization is infected with ransomware, it can be a worst-case-scenario disaster. Recovery may be impossible. So always maintain file backups. Test backups regularly, at least once a month, to ensure they can easily restore lost data.

Limit access to network shares

Many ransomware variants attempt to infect shared network drives. Review all network shares and backup locations. Change their permissions to allow access only by the administrator (and/or the backup service provider). Also, when you need to mount a backup for restore purposes, make sure the permissions are set for read-only.

Install anti-virus

Install a reputable anti-virus on all workstations, such as Avast, Microsoft Security Essentials or Malware Bytes, and use active monitoring.

Patch

Always maintain the latest versions of your firewall, antivirus, operating systems, applications, and other systems. Routinely update as new patches become available, and update automatically if possible.

Educate users

User education must be part of any program meant to prevent ransomware. Highlight the warning signs of suspicious emails and suspicious websites. Demonstrate the need for regular patching and policy review. Encourage users to separate personal web use from their professional web use.

Malicious Emails

Hackers need a way into a business network. One of their favorite channels is email. Why?

First, emails are simple and virtually free to send. Second, almost every organization accepts email – i.e. it's a door that is always open. Third, people of all skill levels – from interns to executives – receive emails, and hackers can count on tricking a few of them.

There are many other reasons why hackers love email, but they boil down to this: email is cheap and it works.

4 Types of Malicious email

Malicious emails come in many forms. The four most dangerous types for small businesses are described below.

Phishing

Phishing is an attempt to trick users into sharing personal details or login credentials. Attackers may do this by encouraging the user to respond to the email, or by asking them to click to a fraudulent website that prompts them to share information.

A link in a malicious email is almost twice as likely to point to a phishing website than to malware, according to research from Proofpoint. The chart to the side compares the monthly count of URLs in phishing emails for all of 2015. [13]

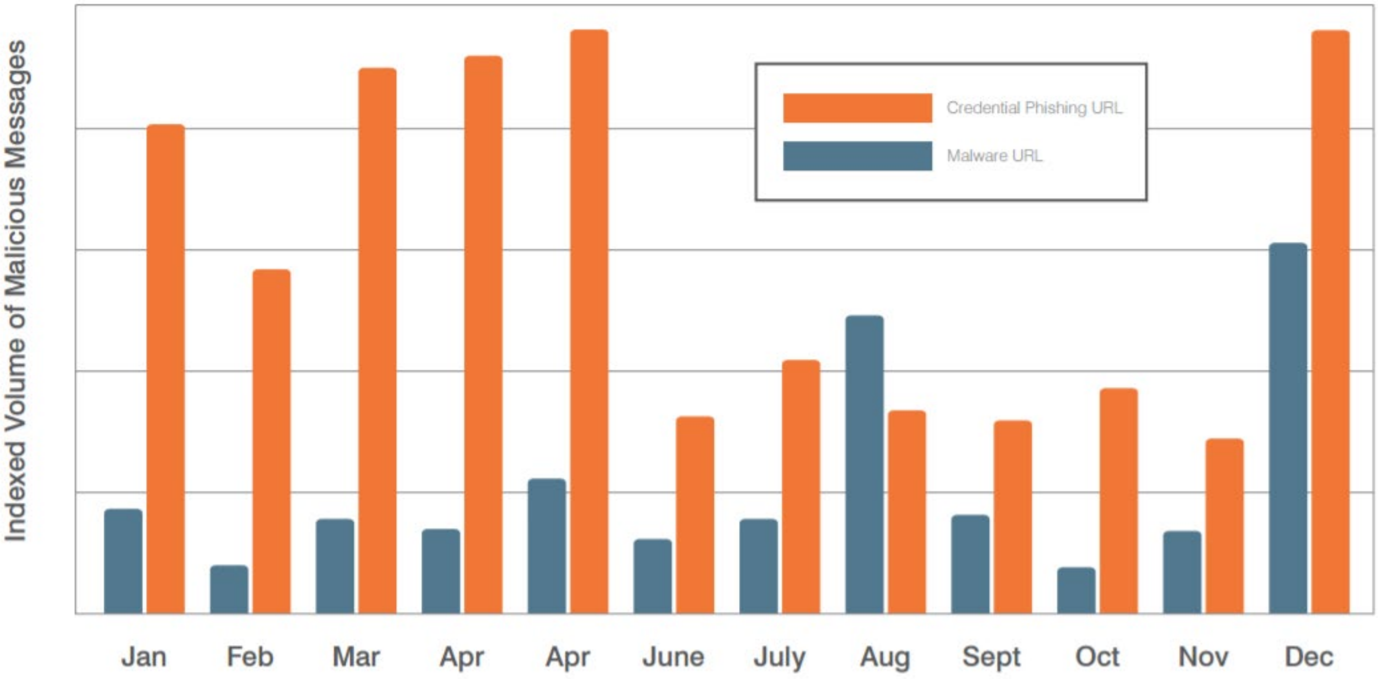


Figure 14: URLs linking to hosted malware vs credential phishing pages, 2015

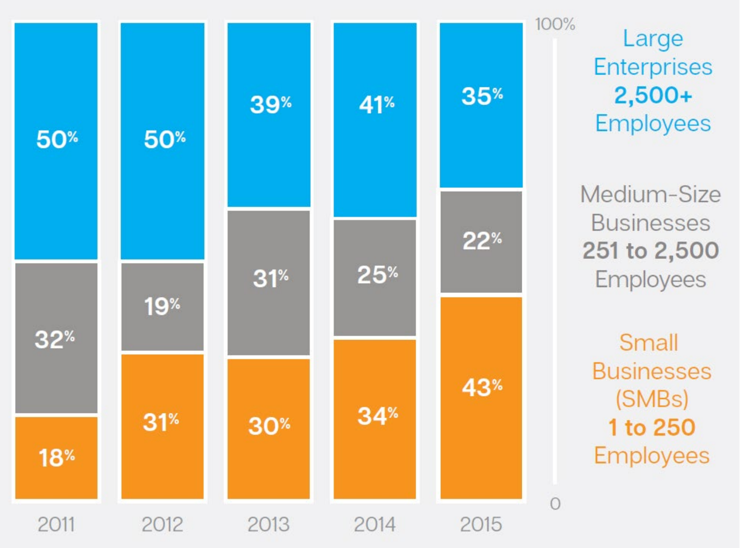
Malicious Emails

Spear phishing

Spear phishing is simply a more targeted form of phishing. Rather than sending a single generic email to a list of millions of email addresses, spear phishing attacks send carefully crafted emails to smaller lists of targets. For example, a fake invoice may be sent to a list of accountants, or a fake real estate market report may be sent to a list of realtors in a specific region.

This approach of sending tailored messages to narrowly defined lists is increasing success for attackers – and increasing damage to small businesses.

The proportion of spear phishing attacks against small and medium businesses (SMBs) has grown every year since 2013. Last year, 43% of all spear phishing attacks targeted companies with fewer than 250 employees, according to this chart from the Symantec 2016 Internet Security Threat Report (ISTR). [14]



Small businesses may not make headlines when they are hit by a phishing attack, but the results can be devastating nonetheless. Data theft, financial loss, and tarnished reputations are just the beginning of a long road that victims can be forced to march.

Malware spreading

Email is one of the most popular ways to distribute malware. Ransomware is often spread through email, as is botnet malware, and spyware that targets banking and other login credentials.

A malicious email will tempt users to install malware typically in one of two ways. The first is with a malicious attachment, often disguised as a Microsoft Word or Excel document or image. The second is with a malicious link.

A malicious email link can take several approaches. It may point directly to the malware and initiate the download immediately. Or it may point to a website that attempts to force the malware on the victim's system secretly (aka "drive by download). Or it may link to a website that disguises the malware as a legitimate download, such as a software update.

Business email compromise (BEC)

This fast-growing threat relies on an attacker's knowledge of the target company. By sending a carefully crafted email, the attacker attempts to initiate a normal business function that will ultimately benefit him.

The most common example is an attack that requests a wire transfer to an account controlled by the attacker. However, attacks can target other business processes, such as shipment of product returns or the purchasing of supplies.

Malicious Emails

BEC attacks often spoof various parts of the email to make it appear to come from a company executive. This is done by forging, for example, the From Name, From Address, and email body. The most powerful attacks compromise the executive's email account outright and use it to email employees directly.

This chart showing the most popular types of subject lines in BEC emails, observed from Q3 2016 by Proofpoint, shows that attackers are often trying to make their messages appear urgent.

One example is an attacker who breaches the email account of a financial executive. By scouring the executive's emails, the attacker may find messages sent to subordinates to request a wire transaction. The attacker can then use the executive's account to send emails to the subordinates requesting a similar transaction, substituting the attacker's bank account as the receiver. The attacker will likely craft the email to use very similar language, style, and timing to be as convincing as possible.

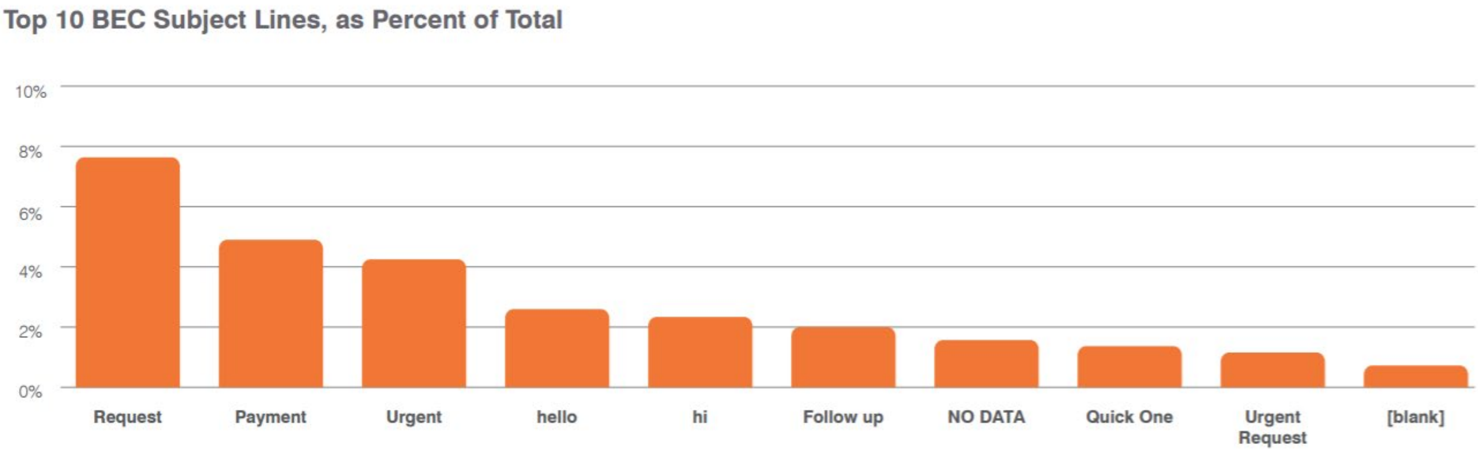

Top 10 BEC Subject Lines, as Percent of Total

Figure 4: Top 10 BEC Subject lines as a percent of total observed incidents, July-September 2016

Malicious Emails

Secure your emails

Small businesses depend on email to communicate with customers and staff members. Though used for decades, the medium shows no signs of dying out. The only viable option is to use email carefully and securely. Tips are listed below.

Train users

Malicious emails prey on the weaknesses of the user. This means an educated user is one of the best defenses against this threat. Even the most tech-challenged staff members can learn to avoid obvious attacks. Train users for constant vigilance when checking email.

Give users a handout with basic email safety tips. Emphasize that they should never click an email that is even remotely suspicious. Also show examples of malicious emails and point out the red flags that should tip off users to the attack.

Simulate attacks

Test users by creating and sending phishing emails. Link the email to a webpage that tells users they have been phished and gives tips for improvement. Several paid services for this are also available.

Explain the risks

Email is one of the most common channels to launch a cyberattack. Explain to users the potential consequences of a breach of the business network. Mention the costs, including forensic analysis, regulatory fines, litigation, and alerting customers. Smaller businesses can be forced to close after an attack.

Secure file sync and share

Since they are so often used to spread malware, some organizations have eliminated the use of email attachments. Instead, they use a file-sharing system. The file is loaded to a secure server and a link to download the file is pasted into the email.

Filter email for spam and malware

This should go without saying – but be sure to use an effective email filter to remove dangerous and distracting messages from the inbox. The email should be filtered by geography (i.e. if you do not do business in Russia, then you should not receive emails from Russia). Also make use of blacklists and whitelists – explicitly defining who is and who is not allowed to send inbound emails to the company.

Internet of Things

Most small businesses have a few "smart" devices on their networks. These internet-enabled gadgets – such as thermostats, DVRs, and IP cameras – are part of the booming Internet of Things, or "IoT". The emergence of these devices is an exciting time for innovation and technology, but it is creating severe problems for cyber security.

The root of the problem is the poor security found in almost all IoT devices. Many are not created with enough memory or processing power to accommodate security functions. Many also lack the ability to apply firmware updates, making it impossible for the user to patch security vulnerabilities as they come to light. This combination of always-connected and never-secure makes IoT devices the perfect targets for hackers looking to expand their botnets.

Botnets are collections of machines infected with malware designed to give a hacker some control over the machines' behavior.

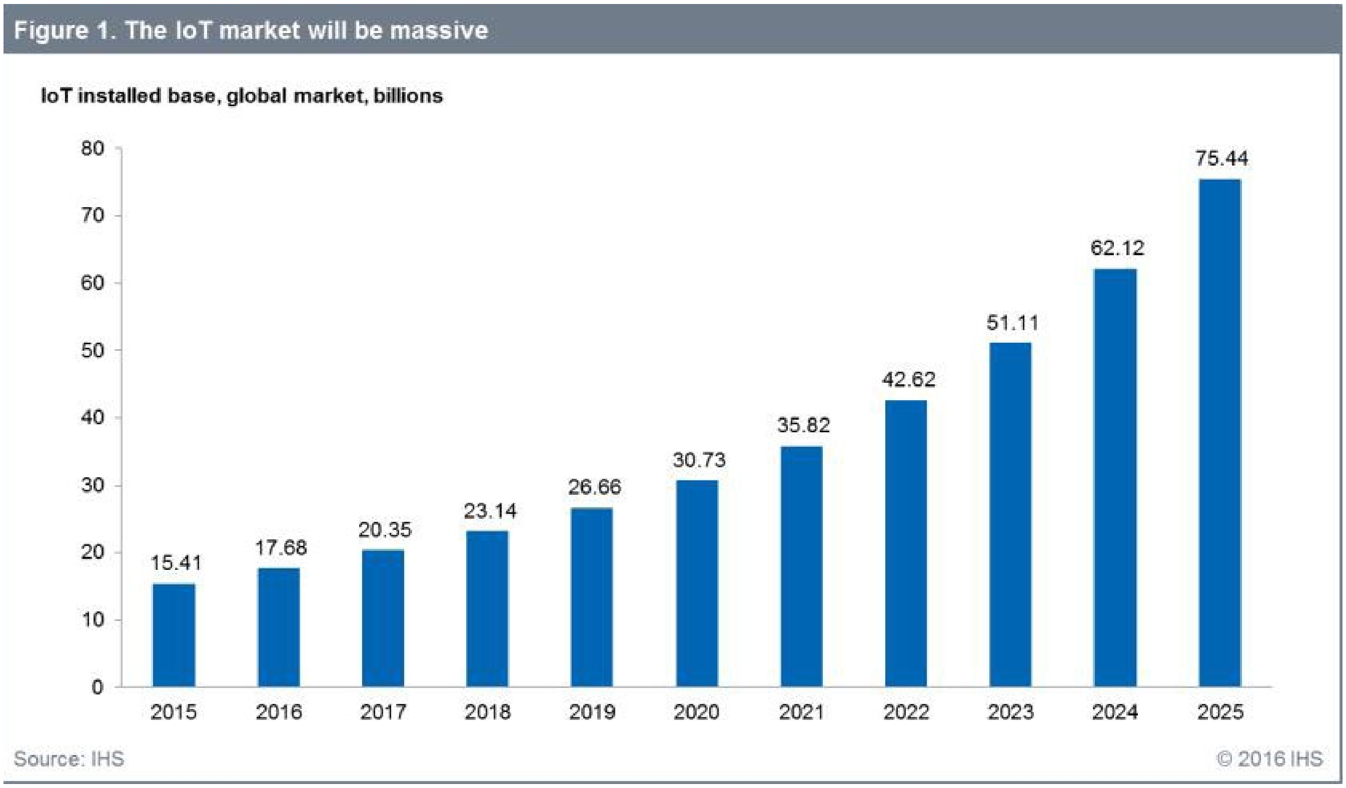
The machines work like a hive of worker bees, executing commands and completing tasks for the hacker, usually without the owners' knowledge. For example, botnets can be used to send massive waves of spam emails. More concerning for small businesses is the use of botnets to launch distributed denial of service (DDoS) attacks and the rapidly growing strength of these attacks fueled by the emergence of IoT.

Billions of 'Things' Online

More than 15 billion internet-enabled gadgets were installed as of 2015. This is predicted to double to 30 billion by 2020, and then more than double again to 75 billion by 2025, according to this chart from analysis firm IHS. [1]

Botnets are piggybacking on this growth.

Figure 1. The IoT market will be massive



Source: IHS

© 2016 IHS

Since billions of these devices connect to the internet with poor security, and billions more will soon follow, hackers are enjoying a botnet bonanza. The result is a massive spike in the strength of DDoS attacks.

Record Breaking DDoS Attacks

Denial of service attacks come in many flavors but the premise is the same. The goal is to render a target unavailable. An attacker floods a target with data in an attempt to consume all of its resources. If the target is overwhelmed, its performance slows or crashes.

A classic example of a distributed denial of service (DDOS) attack is one that uses thousands of computers infected with malware to send traffic to a single target, such as a web server. The volume of traffic overwhelms the server, crashing it, and knocking it offline. This causes a "denial of service" for its legitimate users.

DDoS attacks have been a problem since at least 2000, when a 15-year-old Canadian took out some of the biggest websites of the day, including Amazon, eBay, and Yahoo! [2] The attacks are still launched against networks and web servers every day, and they continue to strengthen.

A recent DDoS attack targeted severs operated by Dyn, a major DNS service provider. Dyn estimates 100,000 endpoints flooded its architecture with traffic on October 21, resulting in congestion and service outages for websites such as Twitter, PayPal, Amazon, and Netflix. [3]

Researchers say the attack was launched from a botnet created by the Mirai strain of malware. Mirai builds botnets by searching the web for vulnerable IoT devices, infecting them, and secretly persisting. The botnet can then be used to overwhelm servers with massive waves of traffic.

Mirai is blamed for several other record-breaking DDoS attacks. In October, Mirai's author poured fuel on the fire by publicly releasing the malware's code, freely giving the weapon to any hacker with the skills to deploy it. [4 5]

Not Just Fun and Games

Hackers join the world of cybercrime for many reasons, but the most common one is to make money. The amount of time and effort needed to create an IoT botnet is substantial, and hackers want a return on that investment.

Below are a few ways hackers may attempt to turn their botnets into cash and how it will impact small businesses.

Extortion

Criminals are making millions of dollars through ransomware, which is a type of online extortion. Experts predict DDoS attacks will soon be used in a similar fashion.

By disrupting an important business service with DDoS, potentially disabling it, attackers can demand payment to stop the attack. While attackers with the best tools are likely to target large companies with deep pockets, less sophisticated attackers with weaker weapons may target smaller businesses with weaker defenses.

Sales

Hackers have created DDoS weapons and sold them for years. A newer trend is to sell them as a monthly service. For a modest fee, a layman can rent a DDoS cannon and fire at will. They even offer tech support and training. Launching the attack is as simple as entering a target and clicking a mouse. This trend will continue to put DDoS weapons into the hands of more people, some of whom will attempt to squeeze money from businesses of all sizes.

Cloud disruption

Small businesses can also expect DDoS attacks to inconvenience them indirectly, such as through the cloud. Customer relationship management systems, websites, email servers, accounting systems, inventory systems – more of these services are hosted in the cloud than ever before. Small businesses love the typically low overhead and high availability these services offer.

However, as DDoS weapons grow in strength and popularity, experts predict cloud and internet infrastructure providers will see more attacks. This can harm the availability of these services for the small businesses who depend on them.

Protect your network

IoT has made a small foray into small business environments. Measures must be taken to ensure these vulnerable devices do not put the organization at risk (and also to ensure they do not become part of a hacker's botnet).

Change default passwords

One of the major flaws in IoT devices is their use of default passwords, such as "admin" and "12345". Always change the password on a device installed on the network. Doing so will help protect it from automated malware strains like Mirai that rely on lazy configurations.

Segment the network

Identify the most important assets on the business network, such as customer data and employee data. Use network segmentation to separate these critical assets from high-risk devices and services on the network, such as IoT devices and guest wifi.

Update the firmware

Some IoT vendors are working to patch security flaws in their devices. Regularly check for firmware updates and apply them. If possible, choose devices that update automatically so patches are applied as soon as they are available.

Any new devices purchased for the company should be required to provide easy or automatic firmware updates.

Reconsider IoT use

Before installing a new IP camera or smart thermostat in the office, ask yourself a few questions: Is this device necessary? What do we gain from it? What do we risk by using it? How can we mitigate those risks? Given all this information, should we install this device on the business network?

Add DDoS protection

Firewalls, intrusion prevention systems, rate limiters, and even dedicated DDoS protection services are just a few of options available to prevent DDoS attacks and minimize the harm they cause. If you are in a high-risk industry or if you have experienced DDoS attacks in the past, then explore these options starting with basic online research.

Vulnerabilities

Vulnerabilities are how hackers breach a system. Sometimes the “vulnerability” is a poorly trained human who recklessly opens emails. However, usually the term refers to software flaws that a hacker can exploit.

Publicly known software vulnerabilities are tracked with the Common Vulnerabilities and Exposures (CVE) system. Each one is recorded with a unique CVE number and stored in the National Vulnerability Database (NVD), which is maintained by the U.S. National Institute of Standards and Technology (NIST).

One of the most reliable pieces of advice to improve security at a small business is to regularly update all systems – all applications, operating systems, firmware, etc.

Applying updates will patch the security flaws that vendors have addressed and defuse an attacker’s attempts to exploit those flaws.

Most Vulnerable Software

The recent growth in non-Microsoft operating systems has paralleled growth in the discovery and exploitation of vulnerabilities in these systems.

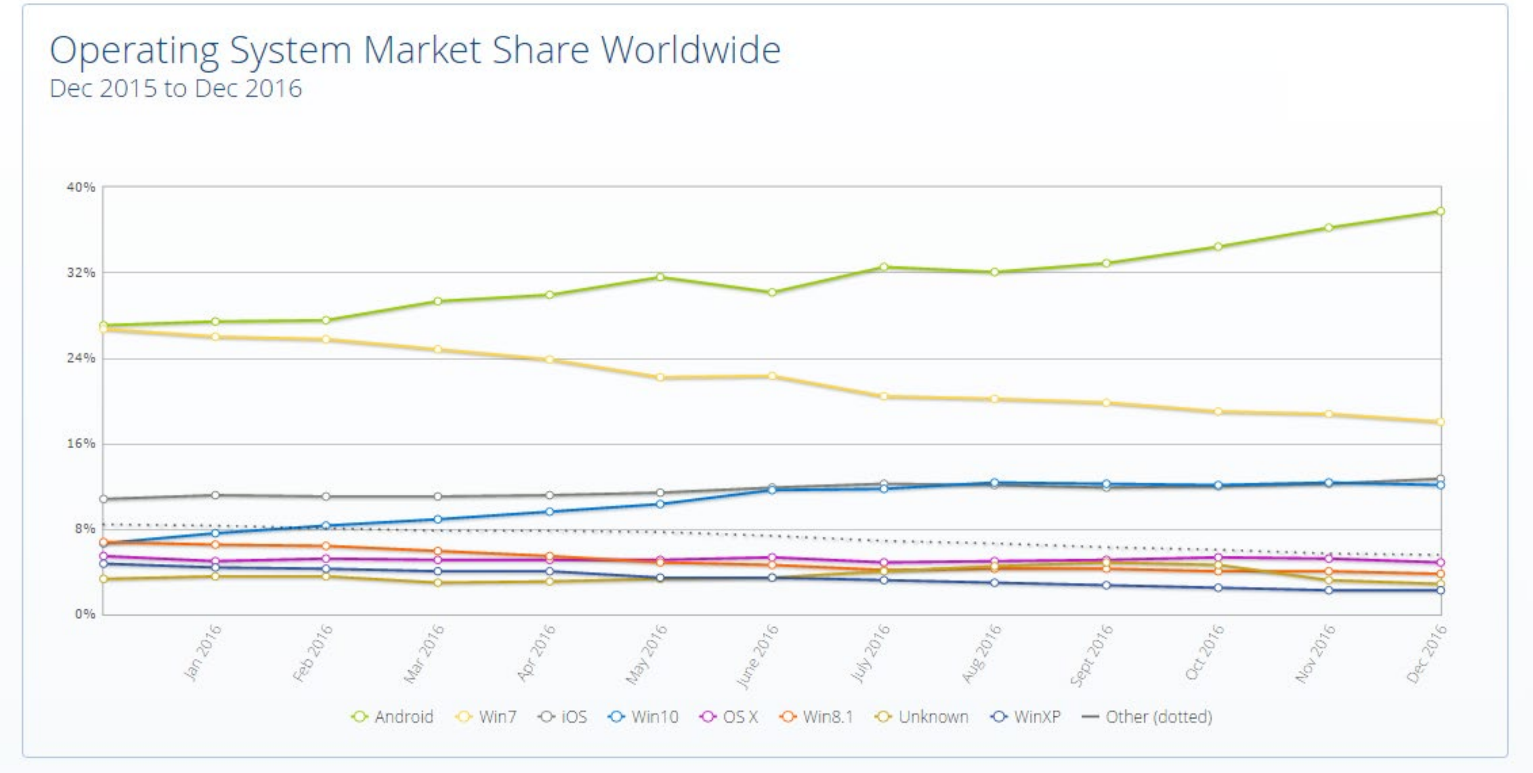
Of the top 10 products that had the greatest number of vulnerabilities disclosed in 2016, none are Microsoft products, according to data from CVEDetails.com shown in the table below. This is a sharp change from 2011, when Microsoft products such as Windows 7 and Windows Server 2003 accounted for six of the top 10. [15]

Top 10 Products by Total # of “Distinct” Vulnerabilites in 2016

Rank	Product Name	Vendor Name	Product Type	# of Vulnerabilities
1	Android	Google	OS	523
2	Debian Linux	Debian	OS	327
3	Ubantu Linux	Canonical	OS	278
4	Flash Player	Adobe	Application	266
5	Leap	Novell	OS	260
6	Opensuse	Novell	OS	228
7	Acrobat Dc	Adobe	Application	227
8	Acrobat Reader Dc	Adobe	Application	227
9	Acrobat	Adobe	Application	224
10	Linux Kernel	Linux	OS	217

Android's lead is not surprising, given that it might be the most widespread operating system in history. Looking across desktop, mobile, tablet, and console systems, Android accounted for 38% of total operating system market share in December 2016, followed by Windows 7 in a distant second place with 18%, according to this chart from StatCounter. [16]

Androids dominance becomes even clearer when looking at the mobile market. For smartphones shipping in Q3 2016, about 87% used Android compared to just 12.5% using iOS, according to IDG. [17]



Vulnerabilities Targeted Most

Vulnerability counts can help determine the risk of using a given product, but they are not the whole picture. For example, Debian Linux had 327 disclosed vulnerabilities in 2016, but hackers are exploiting only a tiny fraction of this number.

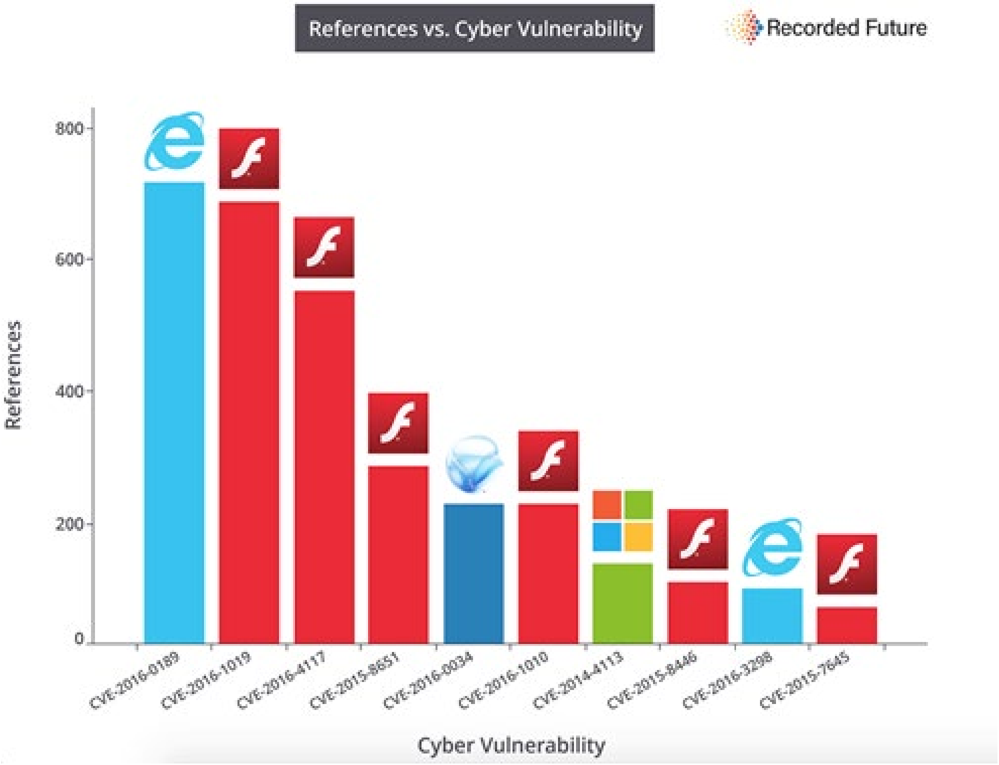
Research on exploit kits may provide an answer. Exploit kits are used to breach a victim's system. They are typically hosted on web servers where they probe the web browsers of site visitors, looking for weaknesses to exploit. The kit then applies the best attack to breach the victim's system. Typically the next step is to install malware.

Threat intelligence provider Recorded Future researched a list of 141 top exploit kits to uncover the vulnerabilities most commonly targeted.

The chart below is based on data from November 2015 to November 2016. While this does not necessarily identify the vulnerabilities most exploited in the wild, it does reveal the weaknesses favored by hacker toolkits, which is a good start. [18]

Microsoft and Adobe are the only two vendors represented in the list. Six of the 10 are vulnerabilities in Adobe Flash, which highlights the pressing need to minimize or eliminate use of this application. The remaining four are for Microsoft Internet Explorer, Silverlight, and Windows.

Adobe Flash has long been a favorite target for hackers and malware to exploit, particularly with drive-by downloads that occur when users browse to a malicious website. Facebook, Google, and Mozilla are just three of many leading tech companies who have announced they will no longer support Flash due to its performance and security problems.



Secure your software

Given all this research, what should small businesses do to protect themselves from software vulnerabilities? These three tips are a great start.

Never use obsolete software

Let's put Windows XP at the top of this list. Administrators should never allow the use of operating systems, applications, or other systems that are no longer patched and supported by their vendors.

Vulnerabilities discovered after software has reached "end-of-life" are not patched by the vendor and cannot be fixed outright. Administrators may be able to mitigate some unpatched vulnerabilities, but this is not a practical solution. The problem will only grow worse with time. Replace the old software.

Always patch systems

The need to patch cannot be overstated. Vulnerabilities are present in all systems. Only by installing updates can these problems be resolved. For many years, the most commonly exploited vulnerabilities were at least one year old. Today, it's more common for exploits to target newer vulnerabilities, but the premise remains: most successful exploits are for weaknesses that vendors have already patched but that users have not applied.

Secure your browser

Look again at the list of 10 most-targeted vulnerabilities. Nine of them are related to a single type of user behavior: web browsing. Users are often the most vulnerable when they are browsing the web (and checking email). Secure browsers by configuring them to automatically apply the newest updates, block the use of flash, and also use ad blocking plugins to prevent drive-by downloads via malvertising.

Software Update

iOS 10.1
Apple Inc.
Downloaded

This update includes Portrait Camera for iPhone 7 Plus (beta), transit directions for Japan, stability improvements and bug fixes.

Bad Habits

One of the greatest threats to network security has nothing to do with software and everything to do with people. It's the users who manage and depend on the network who often put it at the greatest risk.

People threaten security when they make mistakes. This cannot be avoided, but it can be mitigated. Mistakes can be reduced and security can be improved. By correcting bad habits and following a few best practices, a small business can put itself ahead of the curve and out of harm's reach.

Below are some of the worst security habits in small businesses and how to avoid them.

Failing to segment the network

Small business networks have a variety of endpoints. Some engage in high risk behavior, such as visiting disreputable websites. Some are also critically important, such as systems that process or store credit card information.

Too often, a business has everything on the same network with no segmentation. Every endpoint can see every other endpoint. If one system is compromised, they are all at risk.

High-risk and high-value systems should not intermingle on the network. They should be separated, so when a high-risk system is breached (which is all but inevitable) it does not compromise a high-value system and cause serious harm.

To achieve this, the network must be segmented and high-value assets must be isolated. For example, unknown devices connected to a free guest wireless connection should not be able to access the company's accounting and banking records. The network should be segmented to prevent this.

Browsing as the admin

Workstations at small businesses often have one account: the administrator. The administrator can make changes to the system – including the settings for the operating system, applications, and network sharing – without barriers. This is very convenient for users, since they can make changes as needed without hassle.

But this is also very risky. Browsing the web while logged in as an administrator makes it easier for malware to breach the system. Rather than having to ask for administrator privileges before installing, software of any kind (including malware) can install without the user's explicit permission.

A safer approach is to use standard-level accounts on workstations. Standard-level accounts cannot make modifications without entering an administrator password. So if the user visits a website that attempts to force malware onto the system, the operating system will request a password to confirm the action.

A strict approach is to never allow users to have the administrator password. However, this can be very frustrating for some users. Another approach is to require the use of an administrative password to make changes to the system, but to give each user the password. This way, if malware attempts to make a change, the user will be prompted for the password and can refuse to provide it. If the user were logged in as the administrator, this stop-gap would not be in place.

As a side note, do not browse the web on workstations that perform essential functions for the business. If a machine is used to store customer and credit card information, then do not use it to check Twitter and email. Instead, use it only for its primary purpose and limit all non-essential activity on that machine.

Bad Habits

Ignoring email security

Hackers know that almost everyone inside a company receives and sends email (even if it's only with a personal account), and that at least one person can be tricked into opening a malicious attachment or link.

Always filter email for spam and viruses. If you do business only in North America, then block all emails sent from other countries. Use quarantines to allow users to review suspicious emails in a safe, controlled environment. Use blacklists and whitelists to control permitted senders. Also consider using a secure file-sync-and-share system to eliminate the use of email attachments.

Lastly, you must train users to recognize suspicious emails. Hand-outs, presentations, and simulated attacks can help raise awareness of red flags and warning signs. Show examples. Be sure to emphasize the risks so users understand why they must care.

Using outdated software

As mentioned previously, effective security demands the regular patching of all software and systems. Immediately stop using any software that has reached end-of-life and is no longer supported by the vendor with updates. Create a system, even if it's just an item on your calendar, to review and update all software on a periodic basis. Configure systems to update automatically when possible.

Choosing bad passwords

Malware developers count on people to use the default passwords that are identical across thousands of devices. This makes it much easier for them to automate attacks on a mass scale.

Do not make their jobs easy. Never use default passwords, and do not use the same password across multiple systems. Avoid using simple passwords that rely on complete words or simple strings of numbers. Use a mix of letters, numbers, and symbols, and use at least eight characters.

Failing to back up data

One of the easiest ways to overcome a nasty malware infection is to restore the system from a reliable back up. However, many small businesses either fail to back up their critical systems, or they fail to do so effectively.

Automated backups of configurations and data take what could be a labor intensive process and make it hands-free. When possible, store a set of backups offline (off the network and the internet). This will protect them from attacks such as ransomware infections that can scour the available network connections for resources to attack.

Sources

1. HIS: IoT platforms: enabling the Internet of Things (Mar 2016) - https://cdn.ihs.com/www/pdf/enabling-IOT.pdf

2. Wired: Prison Urged For Mafiaboy (Jun 2001) - https://www.wired.com/2001/06/prison-urged-for-mafiaboy/

3. Dyn: Analysis Summary Of Friday October 21 Attack (Oct 2016) - http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

4. DeepDotWeb: Analysis: Record DDoS Attacks by Mirai IoT Botnet (Nov 2016) - https://www.deepdotweb.com/2016/11/06/analysis-record-ddos-attacks-mirai-iot-botnet/

5. Krebs on Security: Source Code for IoT Botnet 'Mirai' Released (Oct 2016) - https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

6. Cyber Threat Alliance: Cryptowall Version 3 Threat - https://cyberthreatalliance.org/pdf/cryptowall-report.pdf

7. CNN: Cyber-extortion losses skyrocket, says FBI (Apr 2016) - http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

8. No More Ransom (Mar 2017) - https://www.nomoreransom.org/

9. Wired: Why Hospitals Are the Perfect Targets for Ransomware (Mar 2016) - https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

10. Becker's Healthcare: Hospitals are hit with 88% of all ransomware attacks - http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html

Sources

11. Osterman Research: Understanding the Depth of the Global Ransomware Problem (Aug 2016) - https://www.malwarebytes.com/surveys/ransomware/?aliId=13242065

12. Osterman Research: Understanding the Depth of the Global Ransomware Problem (Aug 2016) - https://www.malwarebytes.com/surveys/ransomware/?aliId=13242065

13. Proofpoint: The Human Factor 2016 (Apr 2016) - https://www.proofpoint.com/sites/default/files/human-factor-report-2016.pdf

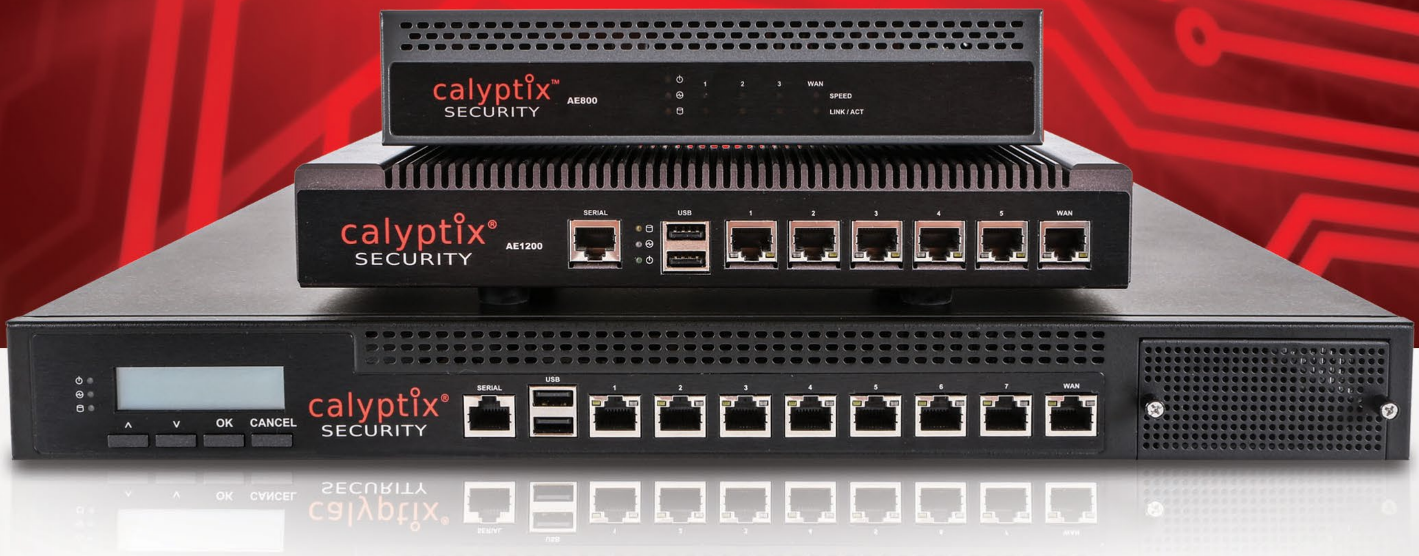
14. Symantec: Internet Security Threat Report (Apr 2016) - https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

15. CVE Details: Top 50 Products By Total Number Of “Distinct” Vulnerabilities in 2016 (Feb 2017) - https://www.cvedetails.com/top-50-products.php?year=2016

16. Global Stat Counter: Operating System Market Share Worldwide (Feb 2017) - http://gs.statcounter.com/os-market-share#monthly-201512-201612

17. IDG: Smartphone OS Market Share, 2016 Q3 (Dec 2016) - http://www.idc.com/promo/smartphone-market-share/os

18. Infosec Institute: Top Ten Vulnerabilities included in Exploit Kits (Feb 2017) - http://resources.infosecinstitute.com/most-exploited-vulnerabilities-by-whom-when-and-how/#gref


calyptix™ SECURITY
AE800
SPEED
LINK / ACT
WAN
calyptix® SECURITY
AE1200
SERIAL
USB
WAN
calyptix® SECURITY
OK
CANCEL