The Top 10 Ways Hackers Get Around Your IT Security

Every day you hear of a new breach at a large company or a government agency. Because these organizations are getting better at protecting their systems. Hackers are now shifting their focus. They are looking at small to medium businesses (SMBs). Why? Because they often do not have the same resources. Think of them as “low hanging fruit” in simply put they are an easy target. Most SMBs are trying to keep up with simple day-to-day tasks let lone cybersecurity. Take steps to not be their next victim. In this short eBook, I will provide you with information from my years of IT security and discuss ways you can be a victim and what you can do to start defending you and your company.

Created by: DK Systems
Patrick Mattson, CISSP, CEH
414-764-4465
info@dk-systems.com
www.dk-systems.com

Whether you realize it or not your company is always under attack by hackers, maybe not physically, but logically. Gone are the days of the kids in their mom's basement playing around and seeing what they can get into. Today there are state sponsored attackers coming after everyone. Countries like Russia and China have teams of government employees who have one job break into networks, they are the new military, think of what they could do to the US if they were able to shut down our electrical grid. These armies of employees are well funded and well trained. In addition to state sponsored attackers, you need to concern yourself with well-funded cybercrime rings that steal and sell your information. Whether you look at yourself as big or small the attacks are the same. In 2022 one statistic I read there were 5.5 billion malware attacks, reference available on the last page. One of the biggest threats to any organization today is ransomware. In a ransomware attack your files become encrypted and the only way to get them back is pay a ransom in a crypto currency or restore from a backup. You are backing your data up, right?????

With that much malware you might think the big companies and government agencies have no issues. Wrong even the biggest of companies and government agencies are under attack and have had successful attacks against them. Some past winners (joking) Home Depot, Target, the IRS, the city of Dallas, the City of Atlanta, the City of Racine, were all hit by some type of attack. This is a small list, there are many, many more. If you read the Wall Street Journal you will read about new attacks almost daily. Before we begin, do you know where all your company data is? I am asking about the data that if was lost could put you out of business or have a big financial impact on you to recover from. Some things to think about: do you have data spread around all the computers or centrally located on a server? Do employees have data on their personal devices? What Cloud services does your company use, are employees using their own to upload files to work on later?

What happens when a hacker gets on to a computer on your network?

- They steal data.
- Encrypt files, making the computer a paperweight.
- They use it as part of bot net, this can be used to attack other computers making it look like your company is attacking them.
- Send out Spam/phishing emails, blacklisting your IP.
- Look for other computers on your network.

Let us look at the top 10 things you can do to help protect your data and network.

1. **Employees are your weakest link: Train employees.**

   So let us pretend you have all the most up to date security tools deployed, whether you installed it, or your current IT provider did. Did you know with one click of a link in an email an employee can launch a ransomware attack?

   Training employees helps them learn to spot "phishing" emails. These are emails disguised as something that seems important. They often have links in them. If an employee clicks on this link, it may not appear anything happened, but behind the scenes malware is running. Phishing emails are the number one way ransomware attacks occur. Train your employees to spot bad emails.

   At the time of this eBook the two most common services offered are Breach Secure Now (BSN) or Know B4. Both offer training videos, quizzes, and simulated phishing emails to train and test employees to spot bad emails. Most MSPs offer this as part of their service, verify your MSP offers this. Currently our service includes Breach Secure Now (BSN).

2. **Patch your devices!**

   This is probably one of the biggest and best tips. I thought about making this number 1. Are you making sure your systems have been patched? Malware is created when hackers learn of a vulnerability, they write the code to take advantage of this. To give you an example, when I spoke at a security conference a few years ago I demonstrated how to take advantage of two vulnerabilities in a Windows 7 computer. One was an older version of Java and the other the computer was missing Microsoft patch MS08-067. In the case of the Java exploit, I had a link that I could click on, or email, and was given full control of the computer, see point 1 about training. In the case of MS08-067 I demonstrated with a few commands how I could create an administrator account on that computer, and I did not need to know the administrator password.

   This is one of the biggest advantages of using a Managed Service plan from an MSP. Our Managed IT service patches systems to ensure everything is up to date.

3. **Backup**

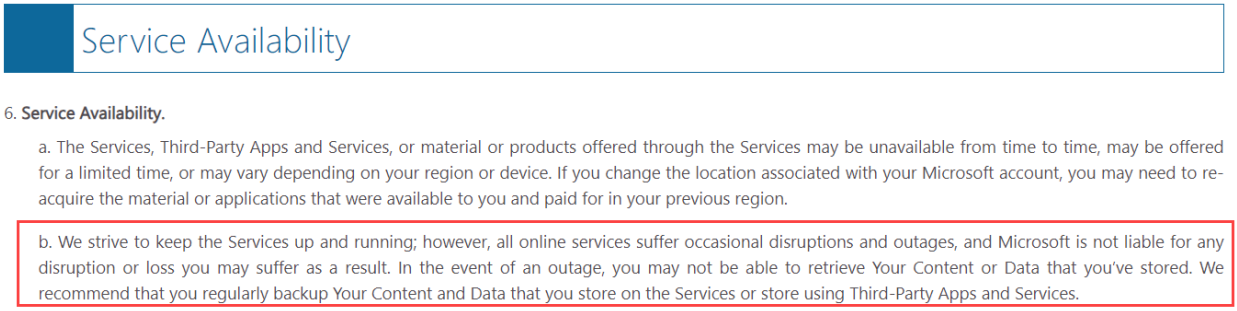
   Backups are the best way to recover from any attacks that might occur. The first question, you are backing up your system(s) now.

   Why do we backup up systems? To recover from a disaster, what are some examples of a disaster? Employees accidentally deletes a file, system crashes, or worse you were attacked. But what happens if something happens to the building? Your backup is in the building that was just damaged, but water, fire, etc. It is important to have an off-site backup. This can be done by rotating drives, cloud-based backups, or your own off-site solution.

   Two quick stories first were I heard about a non-customer in the Milwaukee area had a fire in one of the other tenants' offices. All the units burned to the ground. As a result, their server burned up along with their backup drive. After hearing this we started looking for cloud-based backup solutions

for our customers. In another case one customer had a sprinkler break and got water all over, we could recover the backup drive, but were able to recover from a cloud backup.

How about your email and cloud files? Are you backing those up? You need to verify you are backing up that data too. Microsoft and Google only try to recover files, they do not offer a guarantee. Here is a snippet from the Microsoft agreement we all just agreed to.



Service Availability

6. **Service Availability.**

a. The Services, Third-Party Apps and Services, or material or products offered through the Services may be unavailable from time to time, may be offered for a limited time, or may vary depending on your region or device. If you change the location associated with your Microsoft account, you may need to re-acquire the material or applications that were available to you and paid for in your previous region.

b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.

Most MSPs offer a cloud backup solution to keep your files. At DK Systems we have several options to meet your needs for Microsoft, Google, and on-site solutions.

4. Quality firewall

The firewall is what separates your network from the rest of the world. Its exposure keeps your network safe. Attacks are occurring against it 24x7, home routers are not designed to keep up with the threats. In addition, when you are using a home router you need to keep up with updates to the router, just like a computer it gets firmware updates. Every day new vulnerabilities are discovered in hardware and software. Hackers use automated scripts and bots to scan for these vulnerabilities while we sleep. Our firewall solution is referred to as a Universal Threat Management (UTM) firewall. Here are some of the features:

- Operating system updates
- Intrusion Detection/Intrusion Prevention (IDS/IPS) application. Designed to automatically block any attempts to break.
- A secure virtual private network (VPN) solution to give you and your employees a secure way to connect to your network.
- Optional web filtering, block employees from going to sites they should not, this includes sites know to spread ransomware.

5. Enforce a strong password!

A good password policy makes passwords at least 10 to 12 characters and contains a mix of lowercase and uppercase letters, symbols, and numbers. If you have Active Directory (AD) you can set a policy to enforce a good level of length and complexity. Another good policy is to not use the same password everywhere. Cybercriminals collect and store stolen passwords and credentials, you can even find it on the Internet.

Check out the site: https://haveibeenpwned.com/ you can check if your password has been compromised and it will also let you know where the compromise occurred.

6. **Connect to a safe public WiFi and use a VPN**

   One-way hackers try to get information is setting up fake/cloned WiFi hotspot. Verify with the place you are in and use their WiFi. When connecting to remote WiFi you should do the following:
   - Uncheck the box to Connect automatically.
   - Occasionally review your managed WiFi connections and remove ones you do not recognize or do use anymore.
   - When prompted chose the option to not allow others to see my computer. This sets the firewall policy that is enforced on your computer.

   I remember attending a security conference called Def Con a few years back. If you browsed for available WiFi a list of popular WiFi names was appearing, we were nowhere near any of these establishments. They were obviously fake, but if someone had the connection remembered in their list, they would have automatically connected to a hacker's fake network.

   Whenever you are not on your own network whether in the office or at home you should always use a Virtual Private Network (VPN) before transmitting any financial, medical, or other sensitive information on a public WiFi.

7. **Remove unapproved software.**

   Hopefully your company has a policy against employees installing software on their computers. One big way to introduce security issues within your network is when employees download "free" versions of software like Microsoft Office or Adobe Acrobat. Often these are downloaded from sites that may offer free software, but usually include some type of backdoor. Once an employee installs the software, they may have opened a line of communication back to an attackers' network. They have just created a bridge so the hacker can enter your network through that employee's computer.

   It may seem tempting to save a few dollars on software, but it gives the hacker free access to a computer 24x7.

   You should have an inventory of all software installed on all devices.

   In 2023 a flaw was discovered in a software program named: **MOVEit file-sharing software**. This software was used by a lot of organizations, if it was not patched properly the attackers could steal information.

   What would have happened to your network if an employee installed this software and did not update it?

   You have two ways of checking for software. Manually go around and check each computer or set up software to perform an inventory. This is another big piece of what an MSP provides, verify your MSP is offering this. Our service offers this service, and we have the ability to remove it remotely in most cases.

8. **Separate your networks in the office.**

Today we live in a world where if you go into an office, you expect WiFi to be available. When setting up your WiFi do you have a separate network for guests to use?

By giving guests and employee phones their own network, they cannot see information on your server and employee computers. You never trust someone's device!

The WiFi that has access to your server should:

- Enable WPA2 or higher, be careful with this setting some devices cannot communicate with WPA3.
- Have a strong password that should not be shared with anyone outside of the company. You should change this password occasionally.

Another tip is to create a Virtual Local Area Network (VLAN) this creates logical networks that can run over your existing network. But you can restrict VLANs from seeing other VLANs. This is a little more advanced topic so we will not go into a lot of detail. But often we set up VLANs for: company, guest, VoIP, and WiFi.

9. Sender spoofing the owner's name.

We see this one often and it gets better with training. Employees should question if they receive an email from you asking for something that does not seem like a normal request.

The display name can be spoofed. So, I can send email and put my display name as Bill Gates, but the email might be badguy@example.zzz.

Unfortunately, Outlook does not show the email address. We enable a feature in Outlook to display the email right below the Display Name. One of our customers had a lot of email spoofing to cut down on my calls saying hey the boss emailed me asking for a strange request. They now see the sender's email and know it does not belong to the owner.

10. Policies

Not really a technical control. Policies are considered administrative control. These are your rules for your company relating to IT. Depending on your industry it may be necessary to have policies in place. In some cases, the policies help by telling employees the expectations for using your computers, network, and data. They also list any potential consequences for their actions.

Probably one of the most important policies you should have and have employees sign off on is an acceptable use policy. This basically tells the employees the computer belongs to you, and they should not do illegal things, install their own software, etc. Where this helped one customer is they caught an employee visiting pornographic sites they had the right to terminate them because they signed an agreement stating they will not perform these types of actions on company equipment. Before implementing you may want to run the policy by an attorney or your HR representative to make sure it is would stand up in court.

Other policies may relate to data and agreeing to keep company data confidential and password policies.

We offer a wide range of policies, primarily because several of our customers need to meet compliance standards in different industries and policies are required.

11. Multifactor Authentication (MFA)

This is my extra that I am including. MFA requires two forms of verification. Think of your ATM card. You cannot just walk up to an ATM press a few buttons and get money. You need your bank card and PIN to get money.

In the security world the ability to verify who you are comes in three different methods:

1. Something you know (something in your brain that you know of password, PIN, security questions, etc.)
2. Something you have (something you can physically pick up and hold on to smartphone, badge, etc.)
3. Something you are (think biometric, fingerprint, iris (eye), voice, etc.)

Even if a hacker figures out your username and password, they will need access to your smartphone that contains the authenticator.

Today insurance companies are starting to require their customers to have MFA enabled on anything that allows outside access to your data. This includes remote access to your desktop or server, email, and even sites like SharePoint. In some cases before you can get cybersecurity insurance you need to show evidence this is in place.

Need additional help on these or other IT related issues?

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

There would be no cost or obligation, we will send one of our security consultants and/or a senior technician to your office to conduct a free Security and Backup Audit of your company's overall network health to review. We may need to deploy some tools to gather information, but they will be removed once we are done. From the information gathered we can give a quick assessment of potential gaps in your network. We will review common places that often get overlooked related to security and backups.

Our assessment will give you information on:

- How secure your network is against potential cyber-attacks and if necessary, what you could do to reduce your chances of being a victim?
- Understand what is being backed up and what is being missed.
- Understand what employees are doing on your network.

Let us provide a free assessment!

As a practitioner of IT security, we would like to offer a free assessment of your current IT Security and Backup plan. If you are like me as a business owner, nothing worse than a pushy salesperson. You will not get that with me or my team. We will provide you with a report of our findings and discuss next steps.

Our plans to secure networks vary depending on the customer's needs. For example, if you need to meet a specific standard, a few examples: HIPAA, PCI, CMMC, we may need to add more services. The plan is also based on the number of devices you have. What makes our contract different is we adjust based on the number of devices you have. Some Managed Service Providers (MSPs) lock you with X number of devices even if you go below that level.

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our Free Security and Backup Audit. As a matter of fact.

You have spent a lot of time investing your time and money to get your business started and running it. Like you we have worked hard to obtain our customers and we love to keep them all happy.

Do not risk losing them over a data breach, let us take the stress of IT and protect your data and reputation. Call us at **414-764-4465** or you can e-mail me personally at **patrick @dk-systems.com**

References

Statistics

- Malware attacks in 2022: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/

Articles on entities attacked

- Department of Energy (June 2023) https://www.forbes.com/sites/maryroeloffs/2023/06/15/us-government-agencies-including-energy-department-targeted-in-latest-global-cyberattack/?sh=4dae14802104
- Suffolk County, New York (attack in Sept 2022, article from Feb 2023) https://www.wsj.com/articles/suffolk-county-n-y-restores-systems-after-september-cyberattack-a822f7ee?mod=article_inline
- City of Atlanta (Ransomware March 2018) https://en.wikipedia.org/wiki/Atlanta_government_ransomware_attack

Microsoft agreement

- https://www.microsoft.com/en-us/servicesagreement/upcoming.aspx

Check if a password or mobile number has been compromised

- https://haveibeenpwned.com/