April 2019

TechTidbit.com

brought to you by Tech Experts

Inside The Anatomy Of The Human Firewall

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

Each year, around 61% of small businesses become the victims of a malware attack. While many small businesses may think no one would ever come after them because of their size, know that over half of the total global attacks hit small businesses and, for thieves, getting access to your systems is becoming increasingly lucrative.

Companies collect more about customers than ever before: medical history, financial records, consumer preferences, payment information, and other confidential information.

Some of this information could be used in malicious ways to either harm your business or directly harm the customers, so we all understand that we must protect it from cyberattacks.

Creating a human firewall is the best way to keep your system and data safe, but what exactly is a human firewall, why do you need one, and how can you build one? Let's take a look!

What's a human firewall?

You already know about a "normal" firewall that acts as a technology shield, protecting your primary systems and sensitive customer data from outside threats like viruses, malware, ransomware, and the like.

Protecting your systems with a technology firewall is an important major step to protect your business and customers, but even the most advanced firewalls can be breached because people you trust, your employees, need access to that data in some capacity, putting customer data at risk.

For a timely example, we can look the public relations nightmare that Facebook has endured over the past two years with scandal after scandal related to how they protect the massive amounts of data they collect on users.

In some cases, the data breaches have been related to flaws in the technology; in other cases, people who were in positions to legally access that data made what some consider poor decisions that put Facebook user data at risk.

A human firewall addresses the second part of this. It focuses on risk awareness, training, and monitoring among employees.

It ensures that people and technology effectively work together to safeguard critical systems and consumer data.

How do humans increase your risk?

If you have a firewall, you may be wondering, how can your employees put data protected by a firewall at risk?

Several types of malicious hackers exploit the weakest link in these scenarios and the weakest link, in this case, is the human.

They employ strategies that innocuously coax employees into helping them breach your firewall.

How do they do it? Let's look at two common strategies.

Scenario one: basic phishing scam

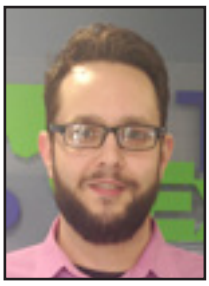
You get an email that appears to be from your boss' boss and it sounds urgent. They say that your boss is not available to help them and they ask you to click on a link and log into a work program that gives you access to customer

Continued on page 4

Several types of malicious hackers exploit the weakest link in these scenarios and the weakest link, in this case, is the human. They employ strategies that innocuously coax employees into helping them breach your firewall.

How Google Password Checkup Can Protect Your Data

"While the hope is that you are protected and that your passwords are all secure, this realistically isn't the case. You can have the strongest password possible, but depending on what information may be sold or accessible, the security can be entirely out of your hands."



Jason Cooley is Support Services Manager at Tech Experts.

While the terminology between a data breach and data leak may not seem very important, being prepared to react to compromised data is. Let's start with knowing the difference between a breach and a leak.

A data breach is an unauthorized intrusion into any private system to access any sensitive data. Data breaches are typically the work of hackers.

A data leak may result in the same end game scenario, but differs greatly in that a leak is data left exposed or accessible, often accidentally.

While the hope is that you are protected and that your passwords are all secure, this realistically isn't the case. You can have the strongest password possible, but depending on what information may be sold or accessible, the security can be entirely out of your hands.

Worse, a breach or leak won't always make national news or show signs of unauthorized access.

If you see an out of state charge on your debit card, you'll have a good idea that you didn't make the purchase and suspect that you've been compromised. In the case of seeing unauthorized charges, the issue is clear.

However, say your email is compromised. It isn't so obvious.

Perhaps the person with your credentials will monitor for a time in order to find valuable information on you or others.

There are so many ways to be compromised and so many types of information that someone with access to your account may be looking for.

In the past, I have used a few different websites to periodically check. This is obviously problematic, as reputable sources for compiling breached information are not overly abundant.

Being an IT professional, I felt comfortable looking for these sources. I do not recommend the same for just anyone.

Luckily, you no longer have to search to find any potentially compromised accounts. Google's new extension "Password Checkup" is here to help.

Google Password Checkup is a browser extension that alerts you to any potentially compromised accounts.

While the browser extension is installed and enabled, it checks any account you log into using Google Chrome.

Now, this is not a foolproof protection blanket. While this is a great tool, it only checks against any data breaches that Google is aware of.

These are the same type of searches I mentioned earlier. While I would have to search before, Google Chrome can handle the work here.

If there is potential that your account is compromised, you should ensure you take steps to recover the account and change the passwords.

While there is no surefire way to remain safe, stay diligent. Remember to make sure your computer isn't compromised by regularly running your antivirus software.

Much like you lock your door at home, make sure you are taking care of your personal information.

Using Google's Password Checkup is a great start, but it's only a start. Change your passwords regularly and keep them unique.

A passphrase is a great way to have a password that is easy to remember but difficult to guess.

Understanding The Value Of Managed IT Services

Depending on their scope and impact on your workday, tech issues can take hours to resolve, if not days. In some cases, you may spend far too much time tracking down a problem, only to come up empty-handed in the end.

In others, such as security breaches, you may not even know there is an issue until the damage has been done.

If you and your team have been handling any tech issues that arise on your own, you could greatly benefit from partnering with a managed IT service provider like Tech Experts.

Here are some of the benefits you can expect from this partnership.

Increases speed of IT repairs

When you partner with Tech Experts, you can report any and all tech issues as they arise and receive a prompt response. Upon receiving your call, we'll look into the problem and find the most effective solution.

With our years of experience, we've probably come across the problem before and already know how to fix it. This makes for very speedy service that helps keep your business operations moving forward without disruption.

Prevents tech issues

Managed IT services prove extremely valuable in the prevention of tech issues of all kinds. From malware attacks to hardware failure, we can stay ahead of the leading issues and potentially keep them from cropping up at all.

Through these preventive actions, you can avoid unnecessary downtime that could otherwise derail the work efforts of your entire staff.

Improves employee productivity

When your employees can hand off tech issues to a dedicated, outsourced team, they can remain on task in fulfilling their daily work duties. This keeps their productivity high, so you can meet your daily business goals and continue to push the annual growth of the company.

With your employees on task, rather than dealing with IT issues, your business operations can continue running smoothly day after day.

Boosts data security

Computer software and hardware issues can have a detrimental impact on the security of your business data. Especially since most of these problems remain hidden from view until a catastrophic loss of data occurs.

Therefore, your company and client information likely remain at risk without help from a skilled IT expert.

We specialize in optimizing security at the network, server and workstation levels, so you can focus on running your business without worry.

Decreases equipment repair costs

You can decrease the amount you spend on upkeep and repair of your equipment with oversight from skilled IT professionals.

Our ability to track down the problem and fix it the first time around will likely prove invaluable as you work on minimizing downtime and boosting employee productivity.

We can also help you time and plan your equipment upgrades perfectly to avoid wasting money on unnecessary items or overspending on parts.

Works well for any budget

With our managed service partnership, you can build your custom IT plan around the exact needs of your company.

You can select the items that will benefit you the most and leave the rest. If you only need computer and cloud support, for example, you can leave all server-related services off your plan. You are not locked into the services you select in the beginning either.

You can also make adjustments to the scope of your managed IT service plan as you expand your operations.

Ability to easily expand

As your business achieves phenomenal growth, you will likely need to add computer equipment and make other key adjustments to accommodate your team and their needs.

We can help you develop a plan that supports your current and future levels of growth. You can build a stronger network, upgrade your software and add computers to your workplace, for example, in support of your company's continued success.

Peace of mind

When you sign up for managed services, you will give yourself true peace of mind in knowing that all your IT needs are handled.

You can call for service any time that your computer equipment acts up or software programs fail to operate as expected.

You will receive support and oversight in the prevention of problems that would otherwise cause much downtime for your employees.

Through all the managed IT service benefits, peace of mind comes out on top as it allows you to focus on what really matters - accelerating the success of your company.

Setting up a managed IT plan

With a look at these managed IT service benefits, it is clear that there are many ways this arrangement can boost the success of your business. You can get started in building this partnership by giving us a call at 734-457-5000. With this call, you can share the network, equipment and other IT needs of your company to start building your plan.

"Computer software and hardware issues can have a detrimental impact on the security of your business data. Especially since most of these problems remain hidden from view until a catastrophic loss of data occurs. Therefore, your company and client information likely remain at risk without help from a skilled IT expert."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(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) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Four Questions Every CEO Needs To Ask About Cybersecurity

Leaders in every organization need to make identifying and addressing their cybersecurity needs a top priority. You can begin by starting a conversation between your IT service company and employees at all levels of your company about information security and how best to protect sensitive data, but you need to know the right questions to ask. Here are four questions to ask to get the discussion started and moving in the right direction.

How informed is your team about the vulnerability to and potential impact of cyber attacks on your company?

It's important to assess the current awareness of everyone in your business about cyber threats and the potential damage from data breaches. It's likely that everyone has heard of the many well-publicized breaches that have occurred over the last several years, but possibly haven't considered them within the context of your company.

This is the first step to developing an educational initiative to get everyone up to speed on the problem and identifying the at-risk areas in your system. After that, you can begin to develop a chain of communication to take immediate action in case of a breach and set protocols and expectations for response times. A fast and effective response is critical to limiting data exposure.

What are the specific risks to your infrastructure and what are the best steps to take to address them?

Remember that the threat isn't limited to just hackers. Many breaches occur because employees click on a link in a phishing email, leave a password lying around where it's easily seen, or by unknowingly becoming a victim of a social engineering scam by giving it to someone over the phone who is impersonating a company employee.

Then you can begin to identify the resources needed to protect your data, including third-party security software and updated equipment. Simply informing your employees of the threat of such low-tech risks can greatly increase your cybersecurity.

How many security incidents are detected in your systems in a normal month or week, what type are they, and how were others informed about them?

You should have a system in place to detect, monitor, analyze, and record any type of potential security incident no matter how small or seemingly insignificant, and disseminate that information to the appropriate personnel, or perhaps to all employees to raise awareness. You should discuss enhanced alerting and monitoring with your IT professionals.

Does your company have an incident response plan? How effective is it, and how often do you test it?

The only way you can quickly react to prevent or limit the damage from a breach is to have a clearly defined response plan in place. It should document how everyone in your company should react in the event of an emergency. This plan should be available to all employees. It should be tested on a regular basis, at least once each quarter, and updated whenever significant changes are made to your IT infrastructure.

Cyberattacks are just a fact of life these days, and that's not going to change anytime soon. But by asking your team the right questions, starting a dialogue about how to address the threat, raising awareness and implementing training, and having a response plan in place, although you'll never completely eliminate them, you can reduce your risks significantly.

Inside The Anatomy Of The Human Firewall, from page 1

information. You click the link and it takes you to a page that looks exactly like your workstation login page.

An employee is caught between a rock and a hard place. It sounds urgent and they could be fired if they don't help their boss' boss.

Because they've been told their own boss is not available, they can't check this out. How many of your employees do you think would comply to avoid getting in trouble? That's exactly why this scheme or something similar to it is so effective.

Scenario two: Spear phishing scam

You get an email that says, "Hi, {your name}, here's the file I promised I'd send you earlier this month. I know you'll find these reports invaluable as a {Job Title}. Let me know how they work for you.". It comes from someone who appears to work in your company or a company that your department often works with, making the email seem valid and trustworthy.

Do you open the file? If you decided to open the file, it just downloaded malicious key-tracking software onto your computer which can now see everything you type, including all of your passwords or it may go further, infecting your computer and those of your co-workers, overtaking your network and stealing data.