Solutions II

THE TOP SECURITY THREATS FOR SMALL AND MEDIUM BUSINESSES IN 2016

IS YOUR TECHNOLOGY PROVIDER PREPARED TO ADDRESS LOOMING THREATS?

THE 2015 SECURITY LANDSCAPE

We are entering an era where more and more of your business will rely on internet-connected systems to function. The rising threat of cyber attacks means that organizations will need to be more focused than ever on security measure like firewalls and anti-virus applications. Companies must also be prepared to recognize and prevent the growing threats that they face from both internal malicious actors and an increasingly sophisticated network of global cyber criminals.

Best-in-class security measures for SMBs must be put into place to ensure security, protect your data, and prevent significant monetary losses.

In this eBook, we'll evaluate the state of IT security for 2015, examine common security gaps in IT plans, and review steps that your business can do to prepare for the future.

CHAPTER 1: THE 2015 SECURITY LANDSCAPE

According to a study published by the professional services organization PWC, only 13% of those surveyed said that they had not experienced a security incident in the last 12 months. 31.5% of respondents stated that they have experienced 50 or more security incidents.

These incidents lead to both employee and customer records being compromised, internal records lost or damaged, and the theft of both hard and soft intellectual property. In addition, respondents indicated that they'd suffered from compromised brand reputation (21.74%), loss of customers (16.82%), and lawsuits (9.61%).

High Profile Hacks of 2015

JP Morgan and Fidelity were among a group of 12 financial institutions that were hacked by cyber thieves, leading to the exposure of the personal information of 100 million people. It has been called "one of the largest and most complex cases of cyber fraud ever exposed."[1]

The US Government's Office of Personnel Management experienced an enormous breach where the records of 21.5 million people were exposed. The information included social security numbers and some fingerprints.[2]

2015 was the "year of the healthcare hack." In one of the largest ever healthcare industry cyber-intrusions, hackers gained access to the data of 80 million former and current members of health insurer Anthem.[3]

[1] Reuters | HYPERLINK "http://www.reuters.com/article/2015/11/13/us-hacking-indictment-outsourcing-idUSKCN0T22E920151113#mL24xiK7Y7dEeelQ.97" http://www.reuters.com/article/2015/11/13/us-hacking-indictment-outsourcing-idUSKCN0T22E920151113#mL24xiK7Y7dEeelQ.97

[2] The New York Times | HYPERLINK "http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=2" http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=2

[3] The Washington Post | HYPERLINK "https://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html" https://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html

Risk for SMBs in 2015

While the hacks of large organizations are the ones that make headlines, the risk for companies in the SMB space is greater than ever.

Let's look at some of the prevalent security issues facing SMBs:

Advanced Persistent Threats (APT) – These are simple attacks where intruders attempt to gain ongoing access to your system without discovery. Often, these are initiated by spear phishing email messages that appear to come from a trusted source.

While many are predicting that these will become less prevalent in 2016, there are a load of hacking techniques ready to take the place of APTs.[4]

Ransomware – Ransomware like OphionLocker and Cryptolocker, continue to be a headache for IT professionals. Unlike APTs, ransomware infects a machine and puts the data on lockdown until a ransom payment is made.

Organizations may view these nefarious sounding viruses as something unlikely to happen to them. However, the FBI says that cyber criminals are netting an estimated $150 million a year off of ransomware.[5]

Malware and Mobile Malware – According to IBM's Security Intelligence site, malware is going mobile. Ori Bach, IBM's Senior Security strategist of Trusteer, wrote that 1.12% of mobile devices monitored by the IBM solution in the first half of 2015 exhibited active malware infections.[6]

Malware like SVPENG is the first of what could be many PC-grade malware threats to mobile devices. With so many BYOD policies in the workplace lacking strong security standards, rise in mobile malware in the workplace is expected.[7]

Point-of-Sale Intrusions – Retailors large and small continue to suffer from these types of attacks. Smaller firms are often the targets of direct, brute-force password guessing. Other common techniques are card skimmers and key loggers, which attempt to capture credit card credentials.

These types of intrusions are painful for SMBs who can suffer from lost revenue, the high costs of finding and mitigating the intrusion, and a loss of customer trust.

[4] ZDNet | HYPERLINK "http://www.zdnet.com/article/security-in-2016-the-death-of-advanced-persistent-threats/" http://www.zdnet.com/article/security-in-2016-the-death-of-advanced-persistent-threats/

[5] Norton | HYPERLINK "http://us.norton.com/yoursecurityresource/detail.jsp?aid=rise_in_ransomware" http://us.norton.com/yoursecurityresource/detail.jsp?aid=rise_in_ransomware

[6] Security Intelligence | HYPERLINK "https://securityintelligence.com/mobile-malware-threats-in-2015-fraudsters-are-still-two-steps-ahead/" https://securityintelligence.com/mobile-malware-threats-in-2015-fraudsters-are-still-two-steps-ahead/

[7] Security Intelligence | HYPERLINK "https://securityintelligence.com/svpeng-mobile-malware-expanding-to-new-territories/#.VaIMV_k_OZA" https://securityintelligence.com/svpeng-mobile-malware-expanding-to-new-territories/#.VaIMV_k_OZA

CHAPTER 2:
TOP REASONS WHY SMBS ARE VULNERABLE

As large companies start to spend more of their time and resources on IT security, smaller companies become increasingly vulnerable. Small and medium businesses are fast becoming easy targets for cyber crime. Why?

- SMBs lack security protocols, and hacks can go unnoticed if proper monitoring isn't in place
- SMBs are so focused on their business that they don't keep up with emerging security threats. Known vulnerabilities are left unpatched, waiting to be exploited.
- Employees do not undergo rigorous security training.
- Employees use bad passwords, and SMBs lack password strengthening protocols.
- Equipment containing sensitive company data like laptops, removable devices, and mobile phones get lost or stolen, and there are no security measure for these events.
- SMBs fail to put even the most basic security measures in place, like anti-virus, firewall, and encryption.
- SMBs lack or have incomplete security policies because they don't think they would be targets of intrusions.

National Cyber Security Alliance research says that 69% of businesses handle sensitive information, including customer data. Yet, 77% of these companies do not have formal written security policies for their employees.[8]

SMBs need to prepare for a threat that is not only growing, but prevalent. The National Cyber Security Alliance also says that "nearly half of all small businesses have been the victims of cyber attacks."[9]

[8] Stay Safe Online | HYPERLINK "https://www.staysafeonline.org/business-safe-online/assess-your-risk" https://www.staysafeonline.org/business-safe-online/assess-your-risk

[9] Stay Safe Online | HYPERLINK "https://www.staysafeonline.org/about-us/news/small-and-midsized-businesses-learn-to-protect-their-digital-assets-during-national-cyber-security-awareness-month" https://www.staysafeonline.org/ about-us/news/small-and-midsized-businesses-learn-to-protect-their-digital-assets-during-national-cyber-security-awareness-month

CHAPTER 3: PREPARING FOR THE SECURITY THREATS OF 2016: PREDICTIONS AND PREVENTION

IT security will continue to be a growing concern for SMBs in 2016 as old threats mutate and new threats emerge. Experts are already predicting what businesses and users alike can expect in 2016.

Prediction: The financial incentives for cyber criminals will lead them to look for new open doors. We predict that new innovations in mobile malware will become an ever increasing threat.

Prevention: A comprehensive security plan must be a part of your BYOD policies. Businesses that put an emphasis on enhanced security protocols and anti-virus for mobile devices will help mitigate the mobile malware risk.

Prediction: Social engineering schemes will continue to plague SMB.

Prevention: Email protection that flags these types of communications before they reach the inbox are a step toward prevention. However, these schemes are often perpetrated over the phone as well. Regular security briefings with your team will not only raise awareness around the red-flags of these schemes, but also help organizations virtually eliminate this threat.

Prediction: The growth of the Internet of Things (IOT) will result in a rapid rise in attempts to infiltrate and overtake our connected devices. As a diversity of devices – from refrigerators and physical security systems to cars – become connected to the Internet, cyber criminals will create ways to monitor, overtake, disable, and hold them for ransom.

Prevention: Companies must create an inventory of all of their connected devices and understand both what kind of data is being collected and where that data is then stored. Businesses will need to be smart consumers when it comes to bringing connected devices into the work environment. Make sure that their security has been verified. Also, make sure that the passwords for those devices are strong and the routes into those devices – like your Wi-Fi routers – are secure.

Prediction: Cyber theft of financial information will increase at small merchants and especially at companies that accept credit cards.

Prevention: Companies that store financial data should employ regular IT security gap assessments from third party experts. This will help companies identify gaps and to build a plan based on their security requirements.

CONCLUSION

STOP PUTTING YOUR BUSINESS AT RISK

The best prevention for IT security in 2016 will be to learn from the security failures of the past. Companies with unpatched vulnerabilities from 2015 are at risk and must take steps to implement better enterprise security.

Companies with Devoted IT Staff: Even companies in the SMB space that do employ people to perform IT security struggle with keeping up. The challenge of staffing people with IT security knowledge, keeping skillsets up to date, and implementing large security implementations are difficult when the IT staff is faced with the day-to-day IT needs of the business. Without focused IT security expertise, companies are bound to have gaps in enterprise security.

Companies with IT Managed Service Providers: Many companies trust the management of their IT services to managed services providers who have knowledge about security challenges, but who are not themselves experts at IT security. SMBs must start to be more selective of their MSPs to ensure that these firms have a deep expertise in data security. SMBs who value their data and require a higher standard of security must look to employ managed services firms who are experts at both identifying vulnerabilities and preventing and remediating intrusions.

Businesses planning for the future need to adapt to the technologies of the future – as well as their own security vulnerabilities.

ABOUT SOLUTIONS II

Solutions II is nationally recognized for world class innovation in virtualization, business continuance and data lifecycle management and IT security. Solutions II assists clients every day, to leverage technologies and services that drive the cost out of IT, while remaining secure. Solutions II's commitment of bringing best-of-breed solutions to clients includes a professional services practice dedicated to increasing customer service levels and decreasing the time and support required for implementations to keep their clients "performing ahead of the curve." Solutions II's Recent Accolades:

- Outstanding Security Partner, IBM
- IBM Beacon Award Winner, "Outstanding Systems Storage Solution"
- IBM Tivoli Business Partner Award for Data Protection Excellence Finalist
- CRN Tech Elite 250

How will these security threats impact your business?

Contact us to continue the conversation.

Contact Solutions II

Solutions II

8822 South Ridgeline Blvd., Suite 205 Littleton, CO 80129
Phone: (303) 796-8393 | Toll-free: (800) 245-2156 | Fax: (303) 796-8399 | www.solutions-ii.com

Premier
Business
Partner
IBM