Talk Nerdy To Me

July 2019

NSA CYBERSECURITY ADVISORY: PATCH REMOTE DESKTOP ON LEGACY VERSIONS OF WINDOWS

This is critical for all networks.

FORT MEADE, Md., June 4, 2019 —
The National Security Agency is urging Microsoft Windows administrators and users to ensure they are using a patched and updated system in the face of growing threats. Recent warnings by Microsoft stressed the importance of installing patches to address a protocol vulnerability in older versions of Windows. Microsoft has warned that this flaw is potentially “wormable,” meaning it could spread without user interaction across the internet. We have seen devastating computer worms inflict damage on unpatched systems with wide-ranging impact, and are seeking to motivate increased protections against this flaw.

CVE-2019-0708, dubbed “BlueKeep,” is a vulnerability in the Remote Desktop (RDP) protocol. It is present in Windows 7, Windows XP, Server 2003 and 2008, and although Microsoft has issued a patch, potentially millions of machines are still vulnerable.

This is the type of vulnerability that malicious cyber actors frequently exploit through the use of software code that specifically targets the vulnerability. For example, the vulnerability could be exploited to conduct denial of service attacks. It is likely only a matter of time before remote exploitation code is widely available for this vulnerability. NSA is concerned that malicious cyber actors will use the vulnerability in ransomware and exploit kits containing other known exploits, increasing capabilities against other unpatched systems.

NSA urges everyone to invest the time and resources to know your network and run supported operating systems with the latest patches. Please refer to our advisory for additional information. This is critical not just for NSA’s protection of National Security Systems but for all networks. In order to increase resilience against this threat while large networks patch and upgrade, there are additional measures that can be taken:

- Block TCP Port 3389 at your firewalls, especially any perimeter firewalls exposed to the internet. This port is used in RDP protocol and will block attempts to establish a connection.
- Enable Network Level Authentication. This security improvement requires attackers to have valid credentials to perform remote code authentication.
- Disable remote Desktop Services if they are not required. Disabling unused and unneeded services helps reduce exposure to security vulnerabilities overall and is a best practice even without the BlueKeep threat.

For more information on NSA cybersecurity, check out NSA’s cybersecurity page.

July 2019

Does Your Business Have A Disaster Recovery Plan

What is your strategy for the aftermath of a terrible storm or aggressive ransomware attack? Likely, you have insurance on your building and your physical belongings like desks and computers and the coffee maker. But what about your data? What about the information stored on your server? Believe it or not, while the server itself may be covered by your insurance policy, everything it contains within its drives is not. For that, you need cyber insurance, which we do recommend, but even that won't help you recover lost data that you need to run your business. While a cyber insurance policy may provide a much-needed payout, it won't magically bring back all of those vital files, information, and software you need to run to your business every day. The more you can control about the future of your business, the better off you'll be in the long run. This is where disaster recovery comes in. Whether it's a fire, a break-in, a storm, or even a disgruntled employee, by putting forth a plan for disaster and the recovery process after the fact, you will be far better off. In fact, disaster recovery is becoming required by more and more business insurance policies. With technology growing so steadily, you should expect your insurance company to demand a written disaster recovery plan sooner rather than later.

Here's what you need to include:

1. **A General Prevention Audit** What are the key assets that need protecting? What are the potential impacts on your business if these assets are compromised? List the ways in which these assets are protected and audited regularly for safety.

2. **Your Recovery Team** In this section, you should outline the management team roles during and after a disaster. Perhaps the CEO calls the insurance company while the VP calls to check on the staff. Make sure these people are trained to know their roles and tasks during a disaster. They will need to know when and how to implement the recovery plan.

3. **Emergency Response** In this section, you will outline which kinds of events require a recovery plan. While a white-out blizzard that's citywide may be a triggering event, a small fire in the break room may not. List an overview of what you consider a disaster, and which recovery plan your team should execute.

4. **Communication Plan** It's best to establish a kind of phone tree for disasters. Nominate a person (and a backup person) in each area of your business who is in charge of reaching out to a specific set of employees.This plan should include a basic safety check on your team members and their neighbors (if applicable) as well as plans for returning to work. Perhaps the office is flooded so employees are asked to work from home. Perhaps the city undergoes a massive natural disaster and some employees need a place to regroup and recover. It's a good idea to include in this section your communication to the media (or on social media). Which disasters require communication with your clients?

5. **Recovery Strategies** Finally, you should include a section on recovery. What needs to be implemented in order for your business to recover from a large fire? Where, if necessary, is your alternate workplace? Make sure to include the number of any vendors you need to notify in order to begin the recovery process. This would include your insurance company, your internet service provider, your IT support, and possibly even your phone provider. While your ISP works towards reestablishing internet in your office, your IT support can assist with your business continuity device to make sure that your clients won't notice a dip in service.

It's important to update this document as often as you can. Anytime you change assets, hire new management, expand your building, etc. make sure you revise your disaster recovery plan. Having a business continuity device as part of your disaster recovery plan is of vital importance. This device can spin up your business (your files, your data, your software, anything, and everything) in the cloud so that you can function as close to normal as possible during a disaster. Your employees will be able to work out of this digital space until your physical one is ready again. Your clients shouldn't even notice a difference.

How does your disaster recovery plan stand up to the industry average? Would you like a free business continuity device? Our Done-For-You Disaster Recovery will give you complete peace of mind that you can be back up and running fast in the event of a major data disaster.

BEFORE THE BREACH

HACKERS ARE HERE!

NEW SKILLS FOR A NEW FIGHT

- 1 in 5 businesses will suffer a cyber breach this year
- 81% of all breaches happen to small/medium sized businesses
- 66% of companies do NOT test their backups
- 60% of companies that lose their data will go out of business within 6 months
- 92% of malware is delivered via email
- 97% of breaches could have been prevented with today's technology

Want to learn more about how to protect your business?

Sign up today for our next Cyber Security Lunch and Learn in September!

www.preferreditgroup.com/beforethebreach

talk nerdy to me

PREFERRED IT EMPLOYEE SPOTLIGHT

Meet Jordan Marks, one of our awesome help desk technicians. Jordan will be celebrating his 2 year work anniversary this August. Jordan did not have prior IT experience, but he is very smart and worked hard to learn the business quickly. He now is a ROCKSTAR at knocking out tickets. Jordan is not afraid to tackle a big job. He is happy to research and figure things out. He has learned a lot in the 2 years he has been with us. He shows initiative daily when working through tickets and he is happy to help with anything we ask. We don't know what we would do without him!

Jordan enjoys playing video games, going out with friends, and traveling. He is working on finishing his tattoo sleeve of traditional Japanese art. Jordan started off in mathematics but decided technology was the field he wanted to pursue.

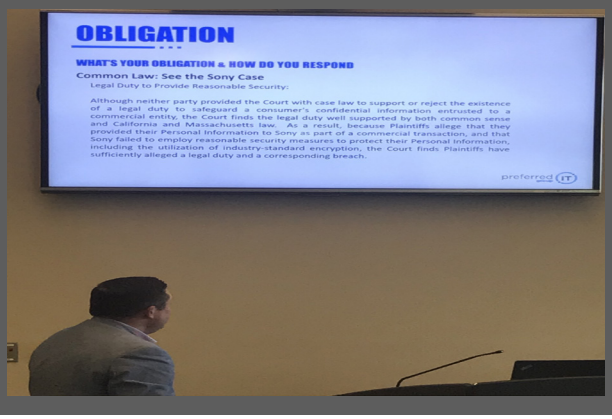
Information Technology

A	I	D	E	M	D	E	B	R	I	D	G	E	D
T	D	R	A	C	S	C	I	H	P	A	R	G	R
E	M	O	N	I	T	O	R	N	E	P	R	O	W
M	O	T	H	E	R	B	O	A	R	D	M	T	M
N	T	E	L	S	S	E	R	A	W	T	F	O	S
E	E	C	A	P	D	L	I	G	H	T	S	R	W
T	T	H	H	O	E	M	N	S	T	W	R	K	I
W	E	N	A	W	S	O	C	A	B	L	E	D	R
O	N	I	R	E	K	U	D	E	B	C	E	I	E
R	R	C	D	R	T	S	N	A	P	P	S	C	L
K	E	I	W	E	O	E	F	O	T	K	D	O	E
R	T	A	A	T	P	S	A	C	R	R	B	N	S
H	N	N	R	A	M	F	C	L	O	U	D	S	S
I	I	R	E	M	H	I	P	T	D	M	A	R	T

MOUSE
TECHNICIAN
RAM
MOTHERBOARD
SOFTWARE
LIGHTS
GRAPHICS CARD
ICONS
MONITOR
DESKTOP
MEDIA
WIRELESS
HARDWARE
CABLE
APPS
BRIDGE
POWER
CLOUD
INTERNET
NETWORK

BEFORE THE BREACH

We had a great turn out for our Before The Breach event this quarter! And we got some new Talk Nerdy To Me swag for the attendees to take home. If cybersecurity is something you'd like to learn more about, give us a call today!



ARCOLA TRACTOR PULLS

This was our third year at the Arcola Tractor Pulls and boy was it a hot one! We want to thank everyone who stopped at our booth and donated to the Arcola Volunteer Fire Department! Every little bit helps and we know they really appreciate the support!

preferred group IT

CONTACT US

Fort Wayne
260.440.7377
Warsaw
574.306.4288
Columbia City
260.213.4266
Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.