ISSUE 26 WINTER 2020

RJ2 TECHNOLOGIES

Newsletter

A Smart Approach to Cybersecurity Investments

Cybersecurity is a threat to businesses across industries. Sometimes, organizations invest in security software without realizing the risks that come with it. Here are compelling reasons why identifying threats before buying cybersecurity products is paramount.

UNCOVER THREATS AND VULNERABILITIES

Every business should run a risk assessment to evaluate its current cybersecurity infrastructure. Doing so is one of the easiest ways to identify, correct, and prevent security breaches. After discovering potential issues that cyberterrorists could exploit, rate them based on probability of occurrence and potential impacts on your business.

Keep in mind that risk assessments are specific to every business, and there is no one-size-fits-all approach for technology that will work for small- and medium-sized businesses (SMBs). Variables like your line of business and operating environment will account for differences in needs and risks. For instance, manufacturing companies and insurance groups have totally different applications to secure.

After tagging and ranking potential threats, identify which vulnerabilities need immediate attention and which ones can be addressed further down the line. For instance, a web server running an unpatched operating system will take precedence over a front desk computer that's running a little slower than normal.

TAILOR CONTROLS TO RISKS

Instead of spending time and money evenly on all systems, focus solutions on areas with high risks. Address these areas' issues immediately after an assessment, but also put plans in place to evaluate their risk profiles more often. This approach is particularly useful to businesses that don't have deep IT budgets but don't want to make security sacrifices.

ASSESS EXISTING CYBERSECURITY PRODUCTS

Chances are, your organization has already spent a great deal of money on purchasing and maintaining various security products. By conducting risk assessments more often, you can improve the strategies you already have in place and uncover wasteful spending. You may discover that one outdated system doesn't really need to be upgraded, or that another legacy technology needs to be ditched. Remember that your existing products were purchased to meet specific needs, and these needs may have immensely changed or disappeared altogether.

Overcoming cybersecurity obstacles becomes easier if you regularly evaluate your IT infrastructure. Contact our experts for help conducting a comprehensive assessment today.

Changes in Windows 10 Update Process

Windows 10 users receive regular security and feature updates for the operating system. But when such patches coincide with driver updates from Microsoft's hardware partners, Windows 10 experiences compatibility problems. Here's how Microsoft is addressing the issue.

First, let's distinguish between driver updates and operating system (OS) updates:

Driver updates – A driver is software that allows your computer's OS to communicate with various hardware devices connected to your computer. Without a driver, the devices you use — display, keyboard, mouse, modem, motherboard, etc. — will not work properly. Hardware manufacturers update their drivers similarly to any standard computer program. Updates are often enhancements to accommodate new software; for example, a new video game with state-of-the-art graphics will require driver updates for your display screen.

OS updates – Windows 10 receives two kinds of regular updates:

Security updates (every month) consist mostly of security fixes that are quickly installed.

Feature updates (every six months) consist of upgrades to the latest Windows version with enhanced features, often requiring multiple reboots to install.

Problems occur when Windows 10 updates are incompatible with a current driver, or when driver updates are released around the same time as Windows 10 updates. In both cases, compatibility issues result in automatic non-installation of updates and startup failures.

To address this issue and improve user experience, Microsoft has changed the way it updates.

#1 MICROSOFT NOW ALLOWS ITS HARDWARE PARTNERS TO REQUEST UPGRADE BLOCKS

Before, Microsoft put up an upgrade block when there were compatibility issues with certain drivers. But now the Redmond-based company is allowing their hardware partners like Intel, RealTek, and others, to request for upgrade blocks if they know their driver is not yet validated. This temporary Windows Update block period is between 30 and 60 days. Once the driver has been updated, then the Windows Update block will be removed.

#2 MICROSOFT BANS NEW DRIVER RELEASES DURING HOLIDAYS AND WEEKENDS

To further improve driver update experiences, Microsoft has banned new driver releases during US public holidays and weekends. This is because Microsoft employees are not available to address compatibility issues that crop up after an update. And Microsoft aims to make driver release dates more predictable in the future.

Do you encounter problems with your Windows 10 updates? If you constantly find it difficult to accomplish the updates for Windows 10 or for your drivers, then you should talk to our Windows experts — they'll be more than happy to assist you. Call or email us right now.

FEATURED PARTNER

Dell

Dell listens to customers and delivers innovative technology and services they trust and value, offering a broad range of product categories, including desktop computer systems, servers and networking products, mobility products, software and peripherals and enhanced services.

RJ2 SPOTLIGHT

Lauren Wood

Account Manager/ Marketing Specialist

Lauren Wood has been in the professional field since 2016. She is a Business graduate from Concordia University - Wisconsin. She started her career in the healthcare field working for Northwest Community Hospital. Before coming to RJ2 she was an account manager at Young Innovations, located in Algonquin IL.

Lauren joined RJ2 Technologies as an intern from 2013-2015. In 2018 she became a full-time employee at RJ2 as an Executive Assistant to the President, Jeff Dann. Now, works as RJ2'S Marketing Specialist and in Account Management.

Fun Fact: Lauren used to study musical theater before finding her career path in Business and Marketing. She also has a St. Bernard Mix called Chubby.

BUSINESS PRESENCE

Office 365 hacking: What you need to know

With over 150 million active subscribers, Office 365 is, unsurprisingly, on top of hackers' minds. And now, hackers are using a technique that doesn't even require users to give up their credentials. Learn how they do it and get protected.

A PHISHING SCAM THAT HARVESTS USERS' CREDENTIALS

The latest cyberattack on Microsoft Office 365 involves harvesting users' credentials. Scammers use this previously unseen tactic by launching a phishing message to users, asking them to click on an embedded link. What makes this scam more insidious than traditional phishing scams is that the URL within the message links to a real Microsoft login page.

HOW DOES IT WORK?

The phishing message resembles a legitimate SharePoint and OneDrive file-share that prompts users to click on it. Once they do, they are taken to an Office 365 login page where they will be asked to log in if they haven't already.

After they've logged in, they'll be prompted to grant permission to an app called "0365 Access." Users who grant permission effectively give the app — and the hackers behind it — complete access to their Office 365 files, contacts, and inbox.

This technique can easily trick lots of users since the app that requests access is integrated with the Office 365 Add-ins feature. That means that Microsoft essentially generates the request for permission. No, Microsoft is not aiding hackers to breach systems. Rather, the scam is made possible by a feature that allows users to install apps that are not from the official Office Store.

WAYS TO PROTECT YOUR OFFICE 365 ACCOUNT — AND YOUR BUSINESS

Given their fairly advanced approach, these scammers could effortlessly prey on careless employees. There are ways to make sure that doesn't happen.

Always check the email's sender account before clicking on any link or granting apps access.

Implement a policy that prevents staff from downloading and installing apps that are not from the Office Store.
Regularly conduct security awareness training that covers essential cybersecurity topics.
Educate employees on how to spot phishing scam red flags (e.g., unknown senders, grammatical and typographical errors, suspicious requests, and the like).
Increase their knowledge about more sophisticated attacks and keep everyone informed about current and future cybersecurity risks.

Successful attacks could result in an unimaginable catastrophe to your company. For tips on how to spot this and other nefarious scams and how to plan thorough security practices, contact our experts today.

Feature Partner Product: Latitude 7490 Laptop

Latitude laptops and 2-in-1s enable all day productivity with the most secure and manageable features all in a beautiful design you will be proud to carry.No matter where work takes you—whether you are on the go, at the desk or working from the café, we have the right solutions so you can office everywhere.

Features:

- 8th Gen Intel® Core™ i5-8350U Processor (Quad Core, 6MB Cache, 1.7GHz,15W)
- Windows 10 Pro 64bit English, French, Spanish
- 4GB, 1x4GB, DDR4 2400MHz Memory
- M.2 128GB SATA Class 20 Solid State Drive
- Ports & Slots

February

"Technology is best when it bring people together" - Matt Mulleweg

TECH TIPS OF THE MONTH

Tips to Writing a better Email:

1. Keep emails short and to the point
2. Make the Subject Line Clear and Concise
3. Make the email personal
4. Remember email isn't private
5. Use plaintext instead of HTML