Devolutions

The Devolutions **CYBERSECURITY GUIDE**

The cybersecurity field is broad and constantly growing. To help you stay on top of best practices, tips, tricks, and warnings, we are pleased to provide this Cybersecurity Guide. It is a curated collection of cybersecurity-related content from our blog. Simply find the topic(s) that interest you and click the links to learn more.

We will be updating this guide on a regular basis, so please bookmark this page and check back often. If you would like us to cover any additional topics, or you would like to become a guest author and share your wisdom and experience with our community, then please contact me directly at dsthilaire@devolutions.net.

SKIP TO CATEGORIES:

THREAT MANAGEMENT

Malware

Before you can protect your devices and organization against malware attacks, you need to know what you're fighting against. Learn about six types of malware, along with best practices for staying safe — click here.

Privileged Account Abuse

Users with privileged account access are given "the keys to the kingdom" — or at least the keys to valuable floors and rooms in the kingdom — so they can be more productive and efficient while carrying out their day-to-day tasks. Unfortunately, privileged users are also prime targets for hackers who want to breach devices and networks, and ultimately steal data. In fact, a survey by Centrify found that 74% of data breaches are triggered by privileged account abuse. Discover what kinds of users are committing privileged account abuse and how to stop them — click here.

Spyware

Spyware – known also as stalkerware – has been around for quite a while. It comes in many forms, from simple tracking cookies to comprehensive surveillance software. Whatever form it takes, spyware is designed for one purpose: to allow the hacker who installed it to learn something about their victim with little regard for that victim's consent or privacy. Learn how to protect yourself and your business from spyware — click here.

Malicious Insiders

The business landscape is full of opportunities and innovations. Unfortunately, it's also full of risks and threats. Preventing insiders from intentionally breaching data will help your organization stay safe by reducing the chances of being victimized by compromised insiders, disgruntled employees, and double agents — click here.

Negligent Insiders

According to the 2019 Insider Data Breach survey commissioned by Egress and conducted by Opinion Matters, 79% of IT leaders believe that in the last 12 months their own employees have accidentally put company data at risk. Even more eye-opening is that 55% of employees who deliberately — but not maliciously — shared data against the rules did so because their company failed to provide them with the necessary tools. Discover how to prevent data breaches caused by negligent employees — click here.

Online Scams

You may be highly aware of online scams — but what about your non-technical colleagues? What they don't know could be very costly to them, and to the company as a whole. Discover seven notorious online scams that your end users need to steer clear of — click here.

Administrative Rights

In the offline world, we don't let just anyone wander around our offices looking into files and opening drawers and cabinets. We have role-based security to keep things safe and secure. However, in the online world, businesses that give everyone administrative rights — usually because it's more convenient to do so — are violating this fundamental security principle and putting their data and reputation at risk. Discover four reasons why giving everyone administrative rights is a bad idea — click here.

RDP

The hack of LabCorp — one of the largest blood testing labs in the U.S. — has raised some legitimate questions about the defense strategies of corporations in an era when cyberattacks can happen at any time. While there are probably many factors that led to the attack, it's worth understanding why hackers are targeting Windows Remote Desktop Protocol (RDP) — click here.

Software Security

ZipCrypto
is supported natively on Windows, but it should never be used because it is completely broken, flawed, and relatively easy to crack. All hackers need to know is 12 bytes of plain text and where it is located in the zip (which can be easily found) in order to decrypt the entire contents of the archive in less than a minute. Discover more about this critical vulnerability and what to do about it — click here.

File Uploads:
User-generated file uploads are essential for many applications and business services. For example, file uploads are a fundamental function for healthcare portals, Content Management Systems (CMS), and messaging applications. However, allowing users to upload files comes with its own set of risks. Attackers are constantly trying to breach systems and steal information by embedding malicious content. Discover how to avoid this type of crisis with proper preventive techniques — click here.

ACCESS MANAGEMENT

Privileged Access Management

The best — and frankly, the only — solution to the growing cybersecurity threat is for organizations to switch from a reactive posture to a proactive one, in which they no longer ask: “What should we do when we get hacked?”, but instead ask: “Since someone is almost certainly going to try and hack us sooner or later, how do we fortify our defenses and stay a step ahead of the bad guys?” The answer to this vital question is for organizations to deploy all six pieces of a comprehensive next-generation Privileged Access Management (PAM) strategy — click here.

Segregation of Duties

Segregation of Duties (SoD) is a policy that forbids a single individual from being responsible for carrying out conflicting duties. The goal, as highlighted in the ISO/IEC 27001 framework, is to reduce opportunities for either the unauthorized or unintentional manipulation or misuse of organizational assets. Basically, when multiple people are involved in a sensitive workflow, there is a smaller chance that anyone will try to break the rules, or for mistakes to go undetected. Learn more about implementing SoD in your environment — click here.

Account Brokering

Resetting passwords is more secure than having the same password permanently available for multiple logins. However, there are some valid security concerns too. Hackers could potentially steal passwords and access accounts before they are reset. And unfortunately, bad actors don't need a lot of time to inflict a massive amount of damage, including creating backdoors to re-enter accounts once passwords have been reset. Discover how account brokering helps reduce this threat — click here.

Privileged Account Monitoring

Organizations rely on privileged accounts to drive productivity and efficiency. Unfortunately, hackers also rely on vulnerable privileged accounts to breach networks, access critical systems, and steal confidential data — often while remaining out of sight for months, or even years. A global survey by the Ponemon Institute on behalf of IBM found that the average time to detect a breach is 197 days, plus it takes an average of 69 additional days to contain the damage. Discover seven types of privileged accounts that your organization must secure and monitor in order to keep your data, reputation, and customers safe — click here.

Zero Trust

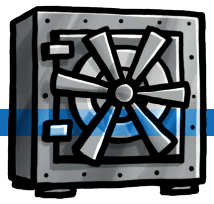
Introduced about a decade ago by Forrester analyst John Kindervag, zero trust is based on the idea that nobody should be automatically trusted — even if they are behind the perimeter or using a trusted network. Instead, prior to accessing parts of the network, users, machines, and apps should be authenticated through technologies such as MFA, IAM, encryption, analytics, and so on. Discover the basics of zero trust along with eight best practices — click here.

Principle of Least Privilege

The principle of least privilege (POLP) is a policy in which end users are given only the amount of access they need to carry out their jobs — nothing more and nothing less. The goal is to minimize the size of the attack surface, and ultimately reduce the likelihood and severity of a cyberattack. Discover more about POLP along with best practices — click here.

Privileged Identity Management

The heart of a robust and functional privileged identity management (PIM) system is determining who should — and just as importantly, who should not — have administrative access to critical systems, since users often have the ability to access secure data, change configurations, install software, modify accounts, and so on. Discover more about this approach along with best practices — click here.



PASSWORD MANAGEMENT

Password Management Best Practices

Strong password management is essential, but also challenging. Discover an updated list of 10 password management best practices that can prevent a costly and potentially catastrophic data breach — click here.

Common Password Security Mistakes

Unfortunately, hackers are finding it surprisingly easy to steal these keys and launch attacks against endpoints and networks. Research has shown that 81% of data breaches are caused by compromised, weak, and re-used passwords, while 29% of all breaches (regardless of attack type) involve the use of stolen credentials. Discover five common password security mistakes and how to fix them — click here.

Don’t Save Passwords in Browsers

As we all know, security is a top priority these days — especially as data breaches become more common, complex, and costly. And if you’re a sysadmin, or you work anywhere in or around SecOps or InfoSec, you also know that end users are usually the weakest link in the network security chain. Unfortunately, browser-based password saver features are usually part of the problem. Discover why saving passwords in browsers is a bad idea — click here.

Good Password Policies

Data breaches are happening all the time, in both big enterprises and even more so in SMBs — which experts view as “ground zero” for cyber crime. As a result, developing good password policies is essential for businesses of all sizes. But it’s not the whole story, because the policies must also be adopted and enforced. That’s why users make the difference between success and failure. Discover five tips to educate your users about good password policies — click here.

END USER MANAGEMENT

Dealing with Security Fatigue

End users have always been (and always will be) the weakest link in the IT security chain. But this vulnerability is made even worse by a condition called security fatigue, which the National Institute of Standards and Technology (NIST) describes as “a weariness or reluctance to deal with computer security.” Discover how to address this particularly dangerous threat — click here.

Safe Online Shopping

We all love online shopping. Sadly, we aren’t the only ones. Hackers love it too, because it gives them a prime opportunity to **hijack accounts, deploy malware, and steal confidential data**, including payment card and bank account information. Discover six tips for safer online shopping during the holidays and throughout the year — click here.

Safe Social Media Usage

Ironically, the same thing that makes social media so popular is also what makes it so dangerous: the belief that people are communicating with people they know — or at least, communicating with people who won't try and hack their device and steal their identity. As pointed out by the New York Times: "The human error that causes people to click on a link sent to them in an email is exponentially greater on social media sites...because people more likely consider themselves among friends." Discover user-focused best practices for keeping social media accounts safe — click here.

Don't Leave Password Management to Employees

Employees who can "manage themselves" are highly valued. After all, nobody wants to (or should want to) micro-manage every little thing an employee does. Micro-managing is not only tedious for everyone involved, but it's inefficient and costly. And frankly, for many SMBs that have limited staff, it's not even an option. However, there are a few functions that shouldn't be assigned to employees regardless of how competent and reliable they are, and at the top of the list is password management. Discover why this is such a big mistake — click here.

Onboarding Employees

Adding a new team member is exciting, and it's always nice to say "welcome aboard" by having a team lunch, assigning a mentor, or viewing an orientation video. However, there are some important things that organizations should do before a new employee arrives. Discover three key cybersecurity tasks to keep in mind — click here.

Offboarding Employees

For all kinds of reasons, turnover is a fact of life. Even companies that routinely make "Best Employers" lists like Google and Costco need to be prepared for when (not if) an employee heads for the exit. Discover five key cybersecurity tasks to keep in mind — click here.

REMOTE WORKING

How to Protect Data at Home

We all know that protecting data at work is a critical priority, since a breach can lead to customer loss, reputation damage, investigation and remediation costs, and possibly even lawsuits, fines, and sanctions. As scary as this sounds, there are ways to reduce the risks of getting hacked, such as using a strong and reliable password management tool rather than a spreadsheet and sticky notes. Discover how to protect your data at home — click here.

Keeping Remote Workers Safe

In the past, remote workers — who were typically called teleworkers or telecommuters — were the rare exception, and the envy of folks who had to endure a miserable commute, or slog away from 9-5 in a tiny windowless cubicle. Well, the situation is radically different today. Businesses must adapt as quickly as possible to survive this unstable and volatile period. These days, remote workers are no longer just a piece of the workforce puzzle, they have become the centerpiece. Discover 10 tips to help remote workers stay safe — click here.

Strengthen Your Home Wireless Network

If you think that your home wireless network is safe and secure out-of-the-box, then think again! On the contrary, it is riddled with default vulnerabilities that could lead to a costly and stressful data breach. What's more, hackers could use stolen information to try and breach your company's corporate network. Discover nine tips to make your home wireless network more secure — click here.

OPTIMIZING SECURITY

Optimizing Data Security in AWS

Although Amazon provides security expertise and infrastructure, you are ultimately responsible for the security of your data. A variety of measures are necessary to keep your data protected from cybercriminals, to comply with regulatory requirements, and to generally keep your information out of harm's way. Discover the AWS shared responsibility model of data security, as well as best practices to help you maximize the security of your data on AWS — click here.

Optimizing Cloud Security

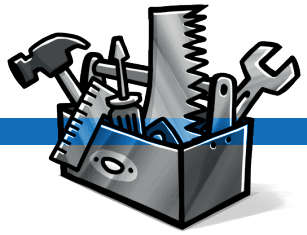
Cloud-based tools help connect disparate business systems end-to-end and drive cross-functional insights. However, because applications generate so much sensitive data, security protocols are crucial. Discover best practices for keeping datasecure in the cloud — click here.

Optimizing File-Centric Security

In today's enterprise, securing your organization's perimeter isn't enough. You need to think beyond your business's walls by considering how remote workers, partners, and suppliers are accessing your systems and data. This involves ensuring sensitive files are always under your control. Discover where to start in that regard — click here.

Developing a Cybersecurity Policy

The best way to ensure valuable information is being protected is by having a solid cybersecurity policy. This is really the first step to making sure your company abides by national and international compliance laws, and is a trustworthy and safe place to store and handle data. Discover foundational tips that will help you develop a strong cybersecurity policy — click here.



TOOLS

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) security provides organizations with the means to monitor, detect, and respond to endpoint threats. Through the application of EDR solutions and practices, organizations gain visibility into the endpoint of the network. EDR also provides organizations with the tools to protect the network against incoming threats as they occur. Learn more about endpoint threats and how EDR technology can keep your workforce and company safe — click here.

Essential Security Tools

We all know that data breaches are on the rise. Which means that most users are increasing their cybersecurity IQ, right? Unfortunately, that's not the case! According to a survey by Pew Research Center, the majority of users are still unclear about some critically important cybersecurity topics, terms, and concepts. To bridge this knowledge gap, discover four security tools that all users must have — click here.

CAREER DEVELOPMENT

In-Demand Roles

According to a survey by Trend Micro, nearly half of all organizations currently lack the cybersecurity specialists they need. And according to research by Gartner, the number of unfilled IT security roles is expected to reach a whopping 1.5 million by the end of 2020. Discover six roles that organizations are struggling to fill, and which (with the right training and experience) you might be an ideal fit for — click here.

Top Certifications

If you're thinking of entering or advancing your career in the cybersecurity field, then smart move — because your skills will continue to be very much in demand. The U.S. Bureau of Labor Statistics estimated a 37% growth rate for cybersecurity (and other information security) jobs between 2012-2022. Discover seven popular and respected certifications that could launch or elevate your rewarding career in the cybersecurity field — click here.

Cybersecurity Skills Shortage

A recent SANS survey has confirmed what seasoned cybersecurity professionals have known for years: the cybersecurity skills shortage is a colossal crater that is growing larger by the day. Discover where the biggest knowledge gaps are and how you can help fill them — click here.

TRAINING

Cybersecurity Training Platforms

A cybersecurity training platform is an online portal that provides employees with self-paced, hands-on, and skills-based threat detection and mitigation training in a live and dynamic simulated environment. Learn more about these platforms and why they are wise (and some say essential) investments for all businesses, including SMBs — click here.

Security Awareness Training

Although a lot of business processes are being taken over by automation and technology, organizations still need humans to take care of most business and customer interactions. The simple and repetitive tasks are automated, but the key decisions still require people. These people comprise the human factor commonly targeted by hackers. To defend against a wide variety of cyberattacks, security awareness training is key. Discover more — click here.

STATISTICS

Cybersecurity Statistics

Forget about script kiddies of the past trying to destroy machines and wreak havoc. Today's cyber criminals are sophisticated, relentless, and well-funded. Here are 20 cybercrime statistics that capture how bad things are, and why security must be the number one priority — click here.