10 Vulnerabilities Hackers Love to Exploit

One PPG Place, Suite 1700
Pittsburgh, PA 15222
(412) 697-5200
www.schneiderdowns.com

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

10 Vulnerabilities Hackers Love to Exploit

Media coverage of data breaches often focuses on the impact, but that's only half the story. What if you could get a behind-the-scenes look at the underlying circumstances that resulted in these breaches?

Schneider Downs' team of cybersecurity experts dedicate significant time and resources into maintaining a detailed understanding of advanced threat actors' current capabilities and methodologies. We leverage this knowledge to help organizations of all sizes and industries improve their ability to prevent and respond to cyber threats.

We asked our team of experts to compile a list of the most common vulnerabilities they have encountered that led to a breach and best practices to mitigate risks going forward.

1. Password Issues

Poor password management and lack of strong password requirements are two of the leading factors in breaches that originate from hackers simply logging on to your systems. Some of the most common shortfalls our team discovers is: the continued use of default passwords; either infrequent or overly frequent password change policies; users setting username as passwords; and yes… we still see the word "password" used. Even with character and capitalization requirements, there are a number of passwords that could meet complexity requirements, yet are still weak passwords. For example, Password!, Steelers2019, and Fall2019 meet Windows complexity requirements but are incredibly simple and guessable passwords.

NIST Password Policy Tips!

- 12 or More Characters / Complexity Requirements (capital letters, special characters, etc.)
- Restrict Common Passwords
- Restrict Months / Seasons / Sports Teams
- Restrict Company-Specific Terms
- Have Passwords Expire Less Frequently (The longer the minimum length, the less frequently you'll need to have a password expire.)

Password Best Practices

- Disable Built-In Windows Accounts
- Use Different Passwords for Accounts
- Remove Administrative Privileges
- Assess How Secure Your Passwords Are
- Password Management
- Employee Training

2. Single-Factor Authentication

Another cybersecurity vulnerability organizations face is the use of single-factor authentication to access company resources over the internet. With a growing virtual workforce, this threat will only continue to grow. This process for securing access to a system—in most cases your network or computer—requires only one category of credentials. In most cases, that's a password.

Cybersecurity Pro Tip!

If your company does not have the means to enable multi-factor authentication through third-party apps, text, or physical tokens, we recommend geo-blocking foreign IPs, if possible, and monitoring and detecting suspicious login patterns through log analysis.

3. Susceptibility to Phishing

Despite all the education around phishing, a 2018 Data Breach investigation found that phishing is still involved in nearly 90% of all data breaches and cybersecurity incidents. To make matters worse, phishing attacks have come a long way since the Nigerian Prince email, which was fairly obvious and contained. New stealth tactics and sophisticated misrepresentation strategies are

making attacks increasingly difficult to identify. With new phishing attacks including complex strategies such as credential harvesting and payload download/execution, mitigating your risk to phishing continues to be a top cybersecurity priority for all organizations.

How to Reduce Phishing Risks?

- Review and purchase the top 10 domains before hackers buy them and start using them against you
- Properly configure spam filters
- Strongly consider employing advanced anti-phishing software (e.g., Mimecast)
- Bolster employee training (simulations, learning modules)

4. Local Administrative Rights

Many organizations are not as restrictive as they should or can be with local admin rights due to technical and/or cultural challenges. Being overly permissive with local admin rights creates an easy target for hackers to exploit and gain control of your company data and systems. How much damage can a hacker do with local admin rights? In many instances, it allows hackers to have remote access, bypass security controls and endpoint protections, and create widespread compromise across your entire network.

Cybersecurity Pro Tip!
Companies should consider restricting local admin rights only to those who absolutely need it, or only on a contingency basis. In the event that the distribution of these powerful rights cannot be avoided, having powerful endpoint protection software to detect common attack techniques becomes a priority.

5. Ineffective Anti-Virus

Experts agree that owning anti-virus software is a best practice in the home and office. But having the anti-virus installed can provide a false sense of security, and hackers prey on that. Despite best intentions, anti-virus software is not an automatic shield from threats due to a number of issues including blind spots with default exclusions leaving files open to attack, signature-based detection which can be evaded by basic obfuscation techniques, and software flaws permitting hackers to simply turn off the software.

Anti-virus Best Practices

- Properly configure anti-virus software to maximize its full potential
- Routinely test and review your configurations and capabilities
- Update definitions automatically upon release
- Consider implementing a next-generation EDR/AV solution (e.g., Carbon Black)

6. Lack of Encryption

When an employee has their smartphone or laptop stolen, hackers have much more than just a new device, they potentially have access to your entire network. The mobility of data and access points are just two reasons why encryption is one of the most critical preventative measures an organization must take to protect itself from the fallout of device loss. Even if the missing device has credential requirements, experienced hackers can bypass those steps and manipulate the data on the device for their own personal gain, or leverage access into your network.

Encryption Best Practices

- Encrypt your databases, either in entirety or specific columns
- Implement built-in TPM endpoint encryption capabilities
- Secure mobile devices with advanced device management tools (e.g., Airwatch)
- Enforce encryption of all USB devices containing sensitive data

7. Data Governance Issues

Do you know where your workers are storing confidential and sensitive data? Have they been trained on which network drives are secure? Are they saving excel files of passwords on their desktop? The truth is, poor data governance puts organizations at risk on a regular basis, with hackers targeting individual devices just as much as a databases and networks. Remember, your company policy is only as strong as those who follow it, and in many cases end users still store sensitive data outside of assigned drives and networks.

Data Governance Best Practices

- Create and communicate data classification/usage policies and procedures
- Enforce governance with software products (e.g., Spirion)
- Routinely audit your end users to identify and remediate policy violations
- Educate your employees on a regular basis, not just during onboarding

8. Flat Networks

Flat networks allow full direct communication with your network, creating an easier target for hackers who look for the easiest way to access a wide range of communication protocols across an entire network. When configuring your network, be sure to prioritize network segmentation, the restriction of any virtual local area networks (VLAN), and establishing local firewall restrictions.

Cybersecurity Pro Tip!

While it may be difficult to change these characteristics in large legacy networks, there are new cutting-edge software tools that make these changes easier. These tools allow for the implementation of software-defined firewalls and micro-segmentation rulesets to be put into place rapidly.

9. Poor Security Monitoring

Are you confident that you can detect a data breach? Even with best practices and software, there are many instances where organizations only realize they're under attack after it's too late. Phishing, password spraying, and widespread rapid use of single-user credentials on multiple systems are just a few of the common undetected hacking activities.

Security Monitory Best Practices

- Ensure that all system logs are being collected and accounted for properly
- Monitor network traffic with effective rulesets to alert on specific activity thresholds
- Ensure specific detection capabilities for each intended attack scenario
- Test your systems with routine attack simulations

10. Unpatched Systems

Unpatched systems are often the root cause of many notable breach scenarios. Patches are released to systems because flaws are identified in those systems. Once those flaws are identified, hackers seek out these unpatched systems on the internet in an attempt to exploit them.

Cybersecurity Pro Tip!

Having a regular patching process that identifies all systems that need to be patched, then installs and verifies that the correct patches have been applied is the ideal scenario. Staying informed of when these patches are released, and building automation into the patching process, are keys to patching success.

BONUS TIP: Physical Security

Why hack a system when you just walk up to it, sit down and access it? Remember, physical security is just as important as digital security and poses the same amount of risk if left unsecured. Be sure to educate your end users on the importance and prevention of physical workspace risks and vulnerabilities. The top physical security breaches our team has encountered include:

- Common Physical Access Control Gaps
- Overly agreeable guards/receptionists
- Unsecured entry ways and network closets
- Unlocked and unattended systems
- Motion sensors that can be hacked
- Security camera blind spots
- Imposter modems and storage devices

Why Call Schneider Downs Cybersecurity Services?

Recent breach reports have outlined the fact that attacks are exploiting security weaknesses faster and easier than ever before and most organizations are not adequately equipped to defend themselves. Schneider Downs can help your organization to be better prepared. We offer a comprehensive set of information technology (IT) security services, including network penetration assessments, network vulnerability assessments, web application security testing, IT security maturity assessments and more. Our team of network security specialists, application configuration specialists, implementation consultants and certified information system auditors can assist your organization with an objective assessment, identifying crucial information and key security risks, and assisting with the implementation of industry best-practice security standards to mitigate these risks.

Cybersecurity services include the following:

- Digital Forensics and Incident Response
- Enterprise Information Security Program Review and Consultation
- External Footprint Analysis
- Firewall Configuration Review
- Incident Response Plan Development, Testing and Training
- Indicator of Compromise Assessment
- Information Security Program Maturity Assessments
- Infrastructure Assessments
- Intrusion Prevention/Detection Review
- MS Office 365 Security Assessments
- Penetration Testing
- Phishing Simulation Exercises
- Vulnerability Assessment
- Web Application Penetration Testing

Contact Us
For more information, contact the Schneider Downs Cybersecurity team at cybersecurity@schneiderdowns.com.

Be in the Know!
Follow our cybersecurity experts on Schneider Downs Our Thoughts On blog for up-to-date insights and advice on cybersecurity issues and developments.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com