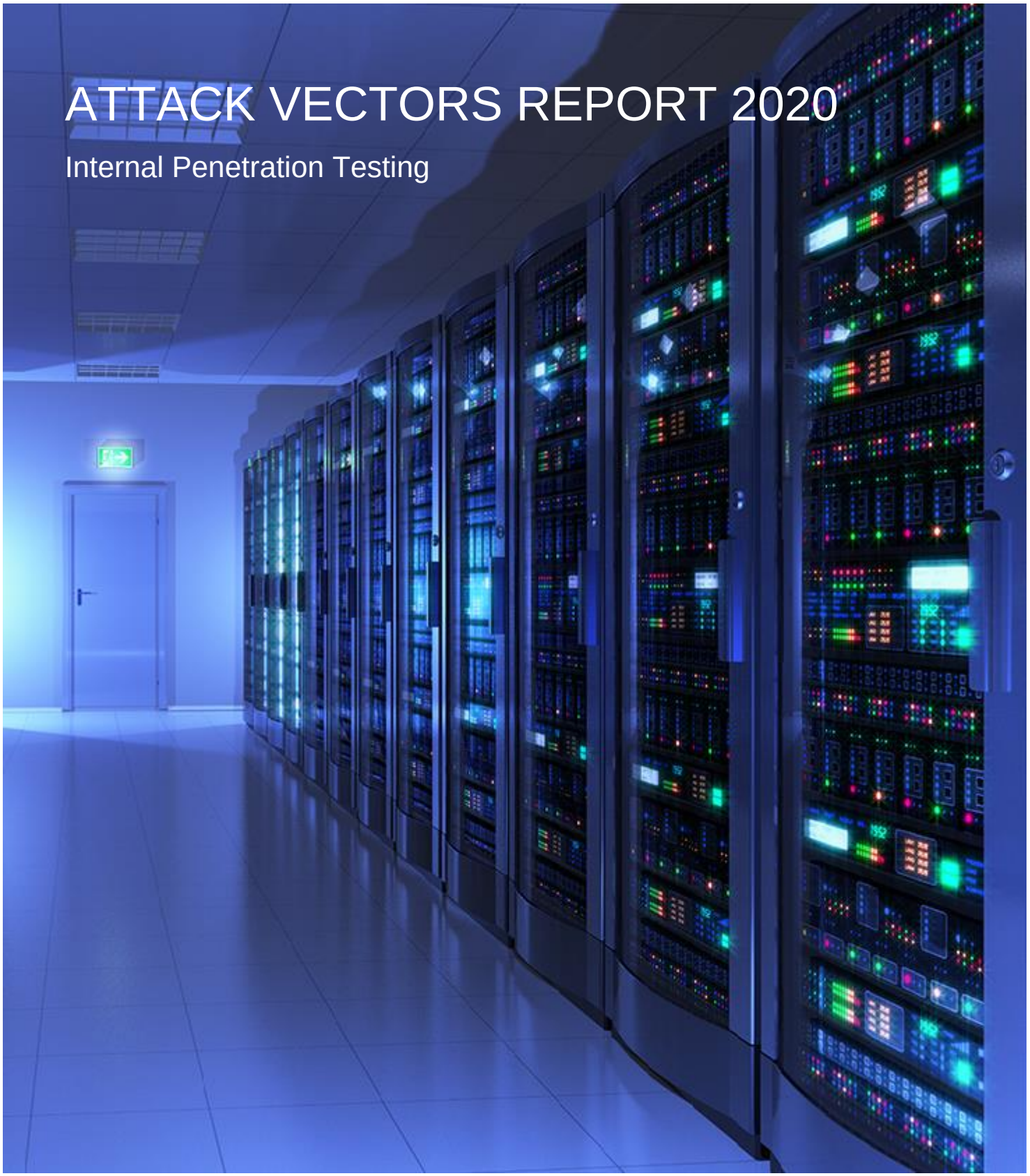
ATTACK VECTORS REPORT 2020

Internal Penetration Testing



RSM

WAR ROOM

Table of Contents

Attack Vectors Report 2020: Internal Penetration Testing

Forward

Each year, as organizations seek to expand in size and revenue, company stakeholders are forced to examine their greatest liabilities. Recent security incidents have proven the development of a new kind of disastrous reality—that of mass data breaching, which can strip an organization of its property without enough evidence to guarantee a successful investigation. From food delivery services to hospitals, any unprepared organization that handles social security numbers, card data, or health information is at risk of experiencing a significant loss.

In order to stabilize the prevention of such incidents, safeguard reputations, and protect sensitive material, many organizations have implemented a multitude of restorative efforts. Because attackers target personal information specifically, it is critical for the affected parties to be aware of any arrangements for "damage control." Immediate identification of suspicious behavior, as well as prompt resolution of any security issue ensures that an organization can remain resilient and protected. However, even the most adaptable organization can find it difficult to master all aspects of information security, while still aligning with internal requirements and regulations.

As part of a continuing effort to assist clients in achieving their desired state of security, while also providing guidance for attack prevention, RSM performs regular security penetration testing. Penetration testing simulates an attack on a network, and closely mimics a security breach without removing an organization's control. In essence, the goal of these tests is to determine what level of compromise an attacker might be able to achieve, and what kind of data they could access.

1. **First, a client with security concerns arranges a simulated attack on their systems by providing RSM with specific subnets for testing.**
2. **We utilize a multi-faceted approach to determine whether internal systems can be compromised without specific credentials.**
3. **Most importantly, we provide clients with the Vulnerability Linkage, which details the sequence of exposures and tactics we use to ultimately lead to a compromise. If an organization is aware of the pathway to compromise, it becomes significantly easier to raise security concerns, discuss risks, and provide high-level guidance to improve the security program.**
4. **Before reporting our methods of attack to the client, we generate a written walk-through of recommendations for the organization. These recommendations are intended to improve the client's overall security, and provide guidance to address the remediation of any discovered vulnerabilities.**

With the cybersecurity industry becoming increasingly specialized, it is crucial that we highlight specific subsets of the attack surface. Inevitably, after performing hundreds of penetration tests every year, we've made note of trends in the vulnerability linkages. These exposures show up time and time again.

For this report, we have focused exclusively on **internal penetration testing**. "Assumed breach" is a common security model, in which controls are tuned with an emphasis on the internal environment. Here, the assumption is that a determined attacker will always find a way into the organization's network. Thus, the vectors covered in our testing all require some level of access to the target's environment.

Executive Summary

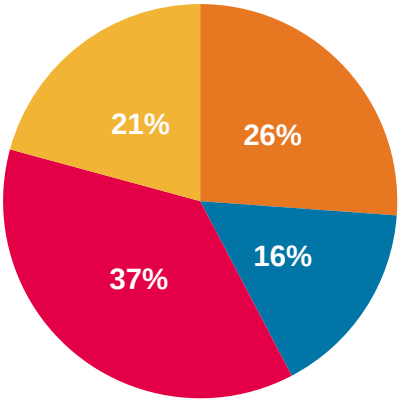
Internal penetration tests simulate an attacker targeting an organization's corporate network. Such attacks can mimic any scenario, from an external threat actor with a foothold on the network, to a malicious insider. This kind of testing is very important due to the increased level of trust typically afforded to people and resources inside the organization.

Over the past two years, we've studied our most successful attack vectors in detail with respect to internal penetration tests. Below are the trends that have arisen, as well as our key takeaways from this analysis.

62% of RSM's internal penetration tests have resulted in a compromise. This means that we were able to enter critical systems and data for the majority of companies we tested from an internal perspective.

At first glance, misconfigurations, such as unnecessary protocols, default configuration or information disclosure vulnerabilities account for the largest share of first steps to network compromises. **Misconfigurations made up 37% of all successful attacks over the past two years.** When correctly utilized, these exposures typically provide multiple pathways to compromise. However, in reality, **the majority of top attack vectors were password-related.** Weak user passwords and NetBIOS spoofing, an attack technique that requires an attacker to crack captured password hashes, combined to account for 47% of total internal compromises. This indicates that many companies are still not educating users on the benefits of strong passphrases, and the dangers of not protecting information in an adequate manner. Weak passwords and protocols that require password cracking are the easiest to exploit, as they can provide immediate entry into the internal network.

Overall Attack Vector Breakdown by Percentage 2018-2020



For the purposes of the following report, we assume the following definitions:

- **Vulnerability:** Any factor which exposes the confidentiality, integrity, or availability of data or systems to a threat. Though vulnerabilities represent security weaknesses, not all vulnerabilities can be exploited in meaningful ways.
- **Attack vector:** A vulnerability whose successful exploitation is instrumental in a compromise. Attack vectors more closely depict the route a threat actor would take in a real life attack. The distinction between vulnerability and attack vector is of great importance because analyzing attack vectors helps organizations understand the potential impact—as well as prioritize the remediation—of exposures in their environments.
- **Compromise:** Obtaining access to critical systems or highly sensitive trophy data.

Important Questions

The following questions should be addressed by organizations once the results of a penetration test have been released.

1. What makes an attack successful?

An attack is successful when a malicious individual obtains access to the internal network. This can be achieved by seizing user credentials or escalating domain privileges. In addition, we consider an attack to be complete if sensitive information, such as Social Security Numbers (SSNs), driver's license numbers or bank information is discovered during the attack.

2. How do attackers identify vulnerabilities?

Attackers can utilize a variety of resources to target and compromise systems, including vulnerability scanning engines and discovery tools. It is important to note that many initial attack vectors are available to individuals without in-depth technical knowledge of cybersecurity and computer systems. For example, attackers can leverage open-source intelligence (OSINT) techniques to explore publicly available websites for employee information. Once an attacker has compiled a list of possible employees from LinkedIn or Google, they can guess email schemas and attempt common passwords to achieve access.

3. Which vulnerabilities should we be most aware of?

After scans are completed, attackers can identify which critical Microsoft patches are missing on the internal network. These patches must be applied by organizations immediately. Exploitation of these vulnerabilities requires little time and no user credentials, and often results in a complete compromise of the victim's machine. In addition, organizations should make an effort to address weak user credentials, as one easy-to-guess password is enough to allow entry to the internal network.

4. What makes a vulnerability "exploitable"?

A vulnerability is exploitable if it allows an attacker to craft a definitive path to compromise. Weaknesses in the network can provide attackers with footholds, or "steps," and can assist attackers in obtaining network details through careful trial and error.

5. What steps do we need to take to prevent attacks, and what resources should we use?

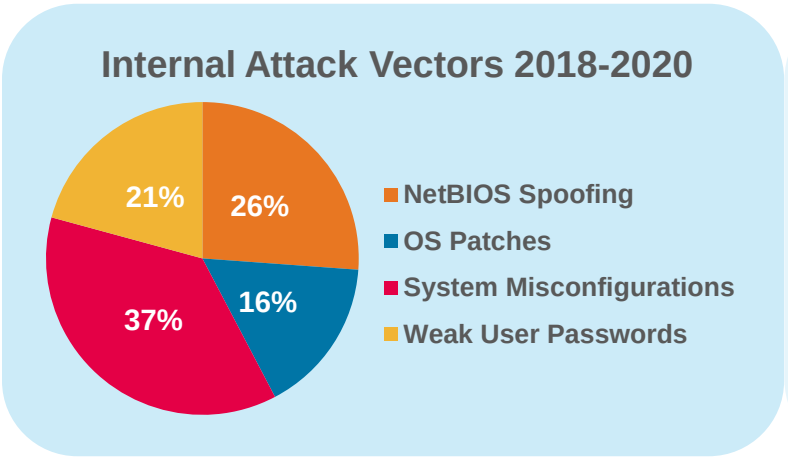
Simple misconfigurations, weak passwords, insecure protocols, missing patches and outdated software must all be examined and remediated to ensure the security of the internal network. In addition, organizations can consider implementing minimum security baselines. Minimum security baselines (MSBs) are available from organizations such as the National Institute of Standards and Technology (NIST) and companies like Microsoft. They provide a standard to which machines should adhere—such as disabling unneeded features or settings and enabling security features that harden the system—which facilitates a consistent approach to system configuration.

6. What is a "culture of security"?

A culture of security refers to the approach that organizations have to cybersecurity, as well as their intentions, awareness, and support of security training. It is not enough for a company to address vulnerabilities and return to their earlier protocol—an organization needs to build a culture of security if they wish to protect information and employee data.

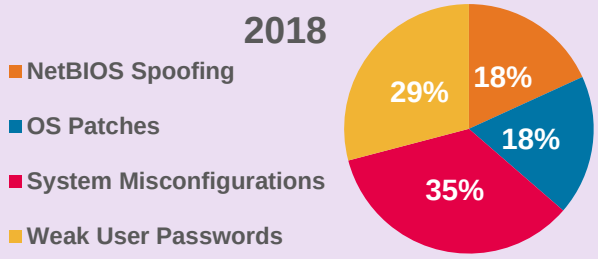
In order to illustrate the success rate of various attack vectors, we have compiled our data from successful compromises into the charts below.

Attack Vectors Overview

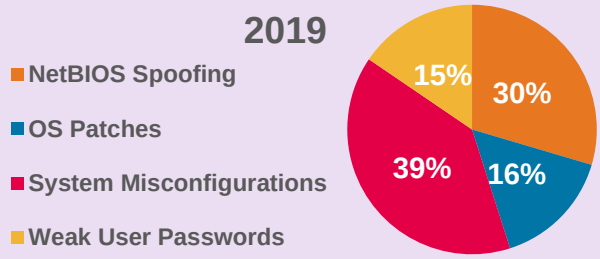


Overall, the majority of our internal compromises between 2018 and 2020 were the result of system misconfigurations. Though minor security issues may not lead to a compromise directly, an attacker with enough time and resources, as well as multiple misconfigurations at their disposal, can craft an attack pathway that utilizes several exploits at a time.

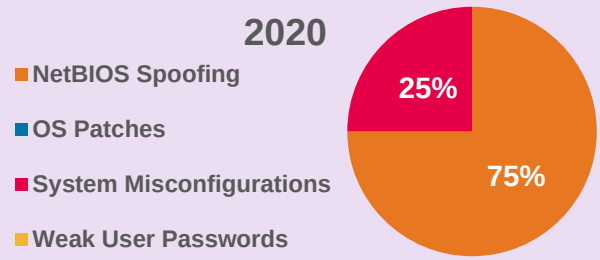
Attack Vectors by Year



In 2018, our most successful attacks were facilitated by system misconfigurations and weak user passwords. When passwords lack length or complexity, or when passwords are repeated across multiple accounts, attackers can more easily brute-force login pages and obtain sensitive user information.



Security misconfigurations were responsible for the highest number of compromises in 2019. These misconfigurations, which can include weak protocols, insecure authentication or encryption, and default system settings can be combined to compromise user accounts.



Though we have not yet concluded our testing for the 2020 year, our data indicates that NetBIOS spoofing is responsible for the highest number of compromises. These attacks leverage default protocols and intercept broadcast requests, which then force victim machines to authenticate to unauthorized systems.

System Misconfigurations (37% of Compromises 2018-2020)

Simple misconfigurations, such as unnecessary protocols or information disclosure vulnerabilities, can provide attackers with a range of information to penetrate internal systems. When utilized correctly, configurations that do not conform to security best practices reveal multiple pathways to compromise. Default setups, unsigned Server Message Block (SMB) protocols and other insecure implementations are included in this category. Most notably, this category contains null session enumeration vulnerabilities, which allows anonymous users to connect to a system and collect its information. As this category encompasses a vast array of attacks and vulnerabilities, the quantity of data attributed to misconfigurations can be misleading.

NetBIOS Spoofing (26% of Compromises 2018-2020)

NetBIOS Spoofing, also commonly called LLMNR poisoning, is a commonly observed default configuration in Windows environments. Link-Local Multicast Name Resolution (LLMNR) and NetBIOS protocols are used to perform name resolution for the names of network computers without certain configurations. When systems cannot resolve host names, a system with LLMNR or NetBIOS enabled will generate a broadcast request, which can be intercepted by attackers who claim to be the resource in question. Once victim machines attempt to authenticate to the spoofed system, they transmit their hashed credentials in the process. If a hashed password is weak enough (or the attacker has sufficient time), the attacker can obtain a valid set of credentials, as well as access to the domain.

This attack is considered reliable and highly successful for internal penetration testing, as it is rarely detected, free and generates quick compromises.

Weak User Passwords (21% of Compromises 2018-2020)

This vector is a catch-all category that includes weak credentials in web applications and email. Weak passwords can allow an attacker direct entry to the internal network, particularly if they lack length or complexity. These passwords can be identified in brute forcing attacks, in which multiple passwords are attempted against one user, or password-spraying attacks, in which a list of weak passwords is attempted against a list of users.

As we occasionally password guess against Active Directory accounts, which are the same kinds of accounts for which we capture password hashes in NetBIOS Spoofing attacks, ineffectual passwords are a significant problem twice over. Combined, these two vectors account for nearly half of all our successful internal compromises.

In order to ensure that a password is strong, predictable or sequential patterns must be avoided. In addition, passwords must not be reused between accounts or applications—if a password is shared between a standard user and an administrator, attacks can progress even further on the internal network. Once entry is obtained, an attacker can easily navigate to sensitive information.

Operating System Patches (16% of Compromises 2018-2020)

Missing operating system patches, specifically for Windows, continue to create significant problems within corporate environments. Because most networks are not effectively segmented, attackers can easily scan a wide range of systems for these easily exploitable vulnerabilities.

It is important to note MS17-010, or “EternalBlue,” in this category. This Windows vulnerability affects the SMB protocol, and was released publicly with a patch in March 2017. When exploited successfully, a

missing MS17-010 patch results in remote code execution as the SYSTEM user, which is the highest level of privilege available locally in Windows. This vulnerability was the most significant starting point for compromises resulting from patch exploitation over the last two years. BlueKeep, a similar vulnerability released and patched in 2019, accounts for a smaller number of compromises achieved by RSM. The missing BlueKeep patch affects the Windows Remote Desktop Protocol (RDP).

Most notably, both MS17-010 and BlueKeep are patchable, and both have been out-of-date for over a year. Organizations without proper asset, change and vulnerability management programs put themselves at significant risk, as flaws like these can appear without warning or fanfare. This makes it very important to ensure patching is done regularly and securely. Any patch that can allow an unauthorized user a direct compromise of the network, or provide the user with a foothold into the internal environment, must be incorporated into an organization's patch management program.

The following chart lists the most common vulnerabilities and exploits identified within each category:

System Misconfigurations
• Default Apache Tomcat configurations • SMB signing not required ("SMB Relay Attack") • Shared local administrator accounts • Man-in-the-middle attacks against IPv6 • Unconstrained Kerberos delegation
NetBIOS Spoofing
• Man-in-the-middle attacks against NetBIOS and LLMNR
Weak User Passwords
• Guessable Active Directory user passwords • Weak internal web application passwords
Operating System Patches
• MS17-010 EternalBlue • CVE-2019-0708 BlueKeep

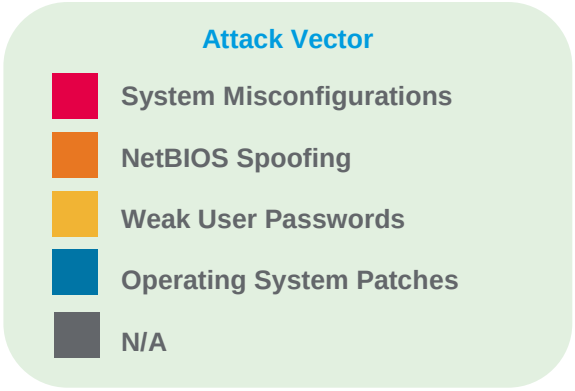
Industry Overview

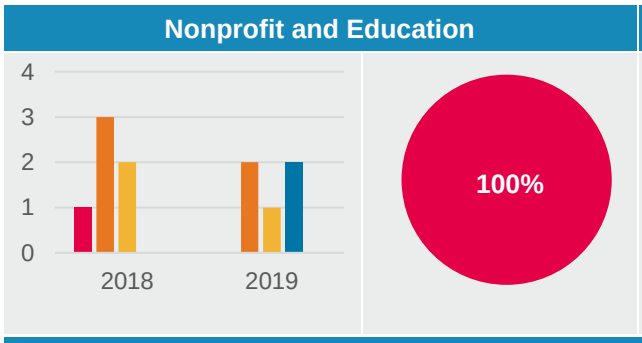
The charts below detail the compromise rate and attack vector breakdown for the five industries in which RSM achieved the greatest percentage of compromise on internal penetration tests:

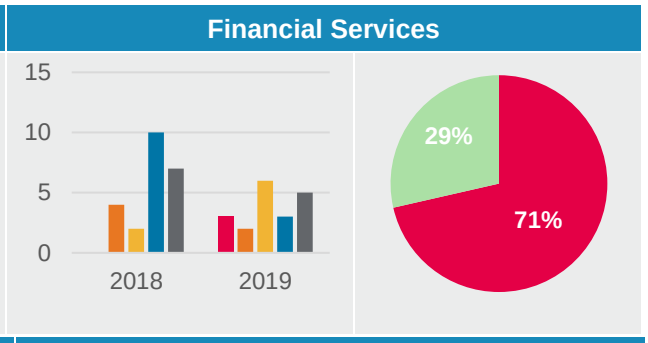
- Nonprofit and Education
- Industrial Products
- Consumer Products
- Financial Services
- Technology

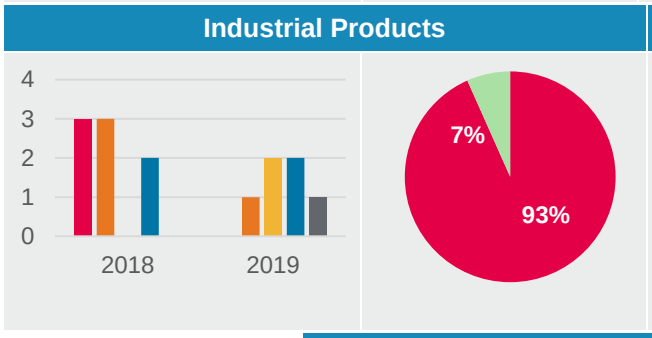
The compromise rates are displayed in order of highest rate to lowest rate, with the Nonprofit and Education clients compromised in every engagement. Overall, system misconfigurations and NetBIOS spoofing have led to the highest number of attacks.

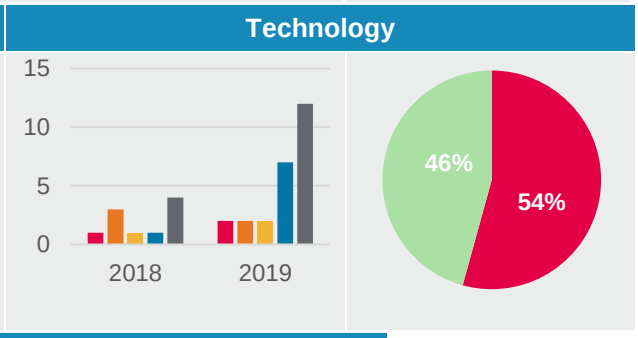
Here, we've chosen to specifically highlight compromises achieved between 2018 and 2019.

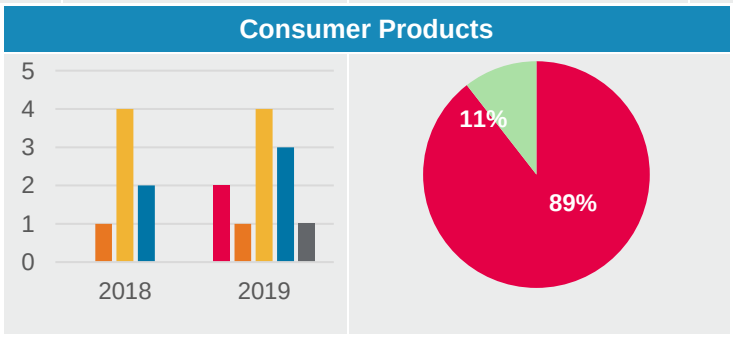












Recommendations

As demonstrated by our findings, network and data security relies on a variety of factors.

The Human Factor

In order to ensure that an organization is protected against future attacks, security awareness and architecture should be emphasized as a means to protect internal networks.

Organizations should assign qualified, dedicated individuals to manage and architect ongoing oversight of security problems. In addition, organizations should conduct regular security training for employees, designed to discuss data protection policies and password strength. Through ongoing awareness campaigns, employees can refresh their knowledge and increase their awareness of security incidents.

Overall, the easiest way to improve an organization's security profile is to prevent simple attacks from occurring in the first place. The items discussed in this report, from weak passwords to missing patches, are easily exploitable vulnerabilities. In other words, these vulnerabilities can be categorized as low hanging fruit that allows potential attackers to take the path of least resistance. Enabling long, complex passwords, ensuring that employees store sensitive information in a secure format, remediating missing patches and updating software are all relatively easy ways to prevent debilitating attacks. Furthermore, making use of multi-factor authentication wherever possible can significantly reduce—though not excuse—the risks associated with weak passwords.

Security misconfigurations and missing patches typically stem from human-centric shortcomings, which include user issues, employee ignorance and organization inaction. Ensuring that employees are trained to spot security problems can help to mitigate risk, and these facets should be included in general security awareness training programs.

The attack vectors in this report provide an overview of exposures and techniques for internal compromise. However, an organization may not know the extent to which their environment is at risk. In order to properly assess their networks, organizations should conduct regular security assessments. Such assessments will effectively leverage the organization's current governance model, internal tools and processes to provide an in-depth analysis of network weaknesses.

Strategic Planning

Over the long term, program level initiatives should be built out based on the same principles outlined above. Vulnerability and patch management programs guarantee that vulnerabilities are addressed in a timely manner without impacting production. Minimum Security Baselines, as previously mentioned in the report, are an organization-wide initiative used to apply device and software security standards to every system on the network. Change management initiatives safeguard network security as devices are added and removed from the network. Organizations of an appropriate security program maturity level should also pursue more targeted planning, which includes Secure Software Development Lifecycles and Security Testing or Audit programs.

Ultimately, organizations should push towards a zero-trust model. Only those individuals with a business case need for data and systems (also known as "least privilege") should be allowed access to these sensitive areas. Unfortunately, though it may feel natural to afford internal resources more flexibility, particularly when it comes to applying best-practice protections, just one misstep can lead to disaster. A company-wide application of least privilege to people, processes and technology can help safeguard the security of the organization and its employees.

Conclusion

Two years of internal penetration testing data have demonstrated that the problems currently plaguing businesses are nothing new. Missing critical Windows patches are a significant issue regardless of whether they are ten years or ten days out-of-date. Internally, the use of poorly constructed passwords continues; NetBIOS spoofing (the exploitation of which depends on crackable passwords) and weak passphrases attached to email, web consoles, and Active Directory accounts led to nearly half of RSM's achieved compromises on internal penetration tests over the last two years.

Internal networks are often treated as a trusted space, and anyone or anything operating within the confines of the corporate network are assumed to be safe. Unfortunately, internal networks warrant just as much monitoring and as many controls as our perimeter networks.

The results presented in this report highlight the continued importance of strong program-level initiatives including security awareness training, asset and change management, and the implementation of minimum security baselines.

We encourage you to more closely examine the vectors presented in this report in order to effectively and efficiently safeguard your internal network environment.

Ken Smith (ken.smith@rsmus.com)
Daria Ryabogin (daria.ryabogin@rsmus.com)

RSM US, Security & Privacy Risk Consulting

Acknowledgements

This report would not have been possible without the efforts of the following individuals:

Daniel Conrad
Erica Cummings
Matthew Franko
John Slusar