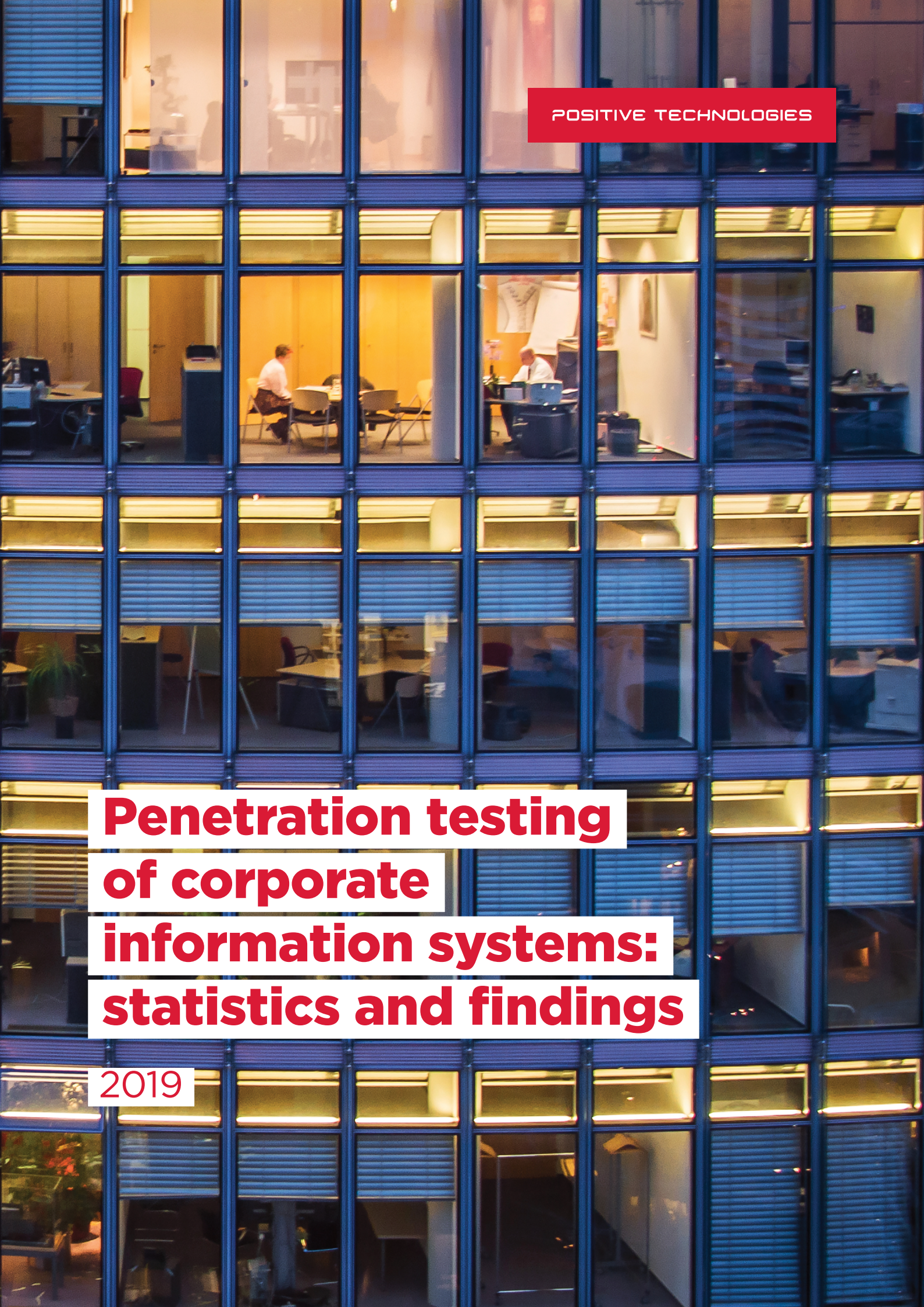

POSITIVE TECHNOLOGIES

Penetration testing of corporate information systems: statistics and findings

2019

Contents

Introduction

A corporate information system is the overarching structure that unites the services necessary for a company to operate. Such systems are complex and constantly changing as new elements appear and existing ones are reconfigured. As the system grows, ensuring information security and defending mission-critical resources from attacks becomes even more difficult.

Security assessment is key for identifying issues with protection of components and spotting potential attack vectors. Penetration testing—by modeling what a real attacker would do against the target system—offers a powerful way to obtain such information. This approach provides an unbiased look at the true level of protection against attacks and shows whether a company's security solutions are effective in practice.

This report presents the results of corporate information system pentesting performed by Positive Technologies in 2018. Based on these projects, the document describes the most common security issues found, practical examples of how these issues might be exploited, likely attack vectors, and recommendations for improving security.

The findings indicated here do not necessarily reflect the current state of other companies. Rather, this information is intended to promote a better understanding among information security specialists of the most relevant issues in a particular sector, as well as assist in timely detection and remediation of vulnerabilities.

Executive summary

Network perimeter testing

- Attempts to breach the network perimeter and obtain access to LAN resources were successful in 92 percent of external pentests.
- At half of companies, an attacker can breach the network perimeter in just one step.
- Vulnerabilities in web application code are the main problem on the network perimeter. 75 percent of penetration vectors are caused by poor protection of web resources.

Internal resource testing

- Full control over infrastructure was obtained in all internal pentesting projects.
- The most common internal network issues were use of dictionary passwords and insufficient protection against recovery of passwords from OS memory.
- Interception of account credentials is exploited with great success in internal pentesting. Among companies at which network traffic was analyzed, not one secured sensitive information from interception.

Staff awareness testing

- One out of three employees risked running malware on a work computer.
- One out of seven employees engaged in dialog with an imposter and disclosed sensitive information.
- One out of ten employees entered account credentials in a fake authentication form.

Wi-Fi security testing

- An attacker would have been able to connect to corporate Wi-Fi networks at all tested companies.
- On 63 percent of systems, weak Wi-Fi security enabled accessing resources on the LAN.

Source data

The dataset for 2018 consists of 33 projects involving testing of corporate information systems for clients consenting to use of such data for statistical purposes. Some projects were not included in order to avoid distortion: tests on very small systems are liable to create statistical noise. Companies represented a wide range of industries, predominantly in the industrial, financial, and transport sectors.

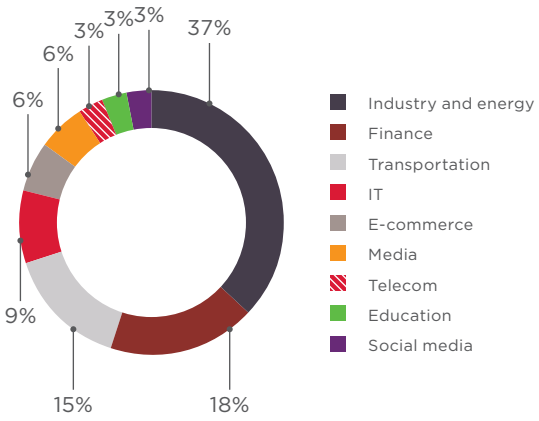

Figure 1. Distribution of tested systems, by industry

Corporate information systems were subjected to external and/or internal penetration testing. By making conditions as close as possible to those of the real world, such testing provides a true measure of the level of security. In external pentesting, testers take on the role of a threat actor who has Internet access but no pre-existing privileges on the target system. Their job is to breach the network perimeter and obtain access to resources on the local network. During internal pentesting, testers are on a segment of the local network and attempt to obtain control over the system infrastructure or critical resources specified in advance by the client. Comprehensive pentesting (internal plus external) was performed at one fourth of client companies.

Wi-Fi security and employee security awareness were performed for a subset of clients.

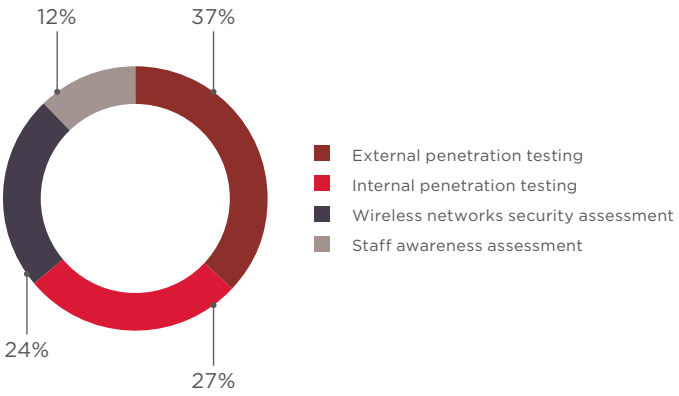

Figure 2. Types of work performed

Overall results

Each vulnerability or shortcoming in protection mechanisms is assigned by our experts to one of four categories:

- Configuration flaws
- Failure to install security updates
- Vulnerabilities in web application code
- Password policy weaknesses

Based on CVSSv3.0, each vulnerability is assigned a degree of risk: Critical, High, Medium, or Low. In keeping with last year's results, almost all systems contained critical vulnerabilities. Most of these related to password policy weaknesses.

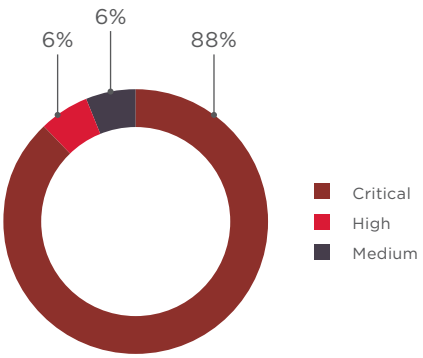

Figure 3. Most dangerous vulnerability found (percentage of systems)

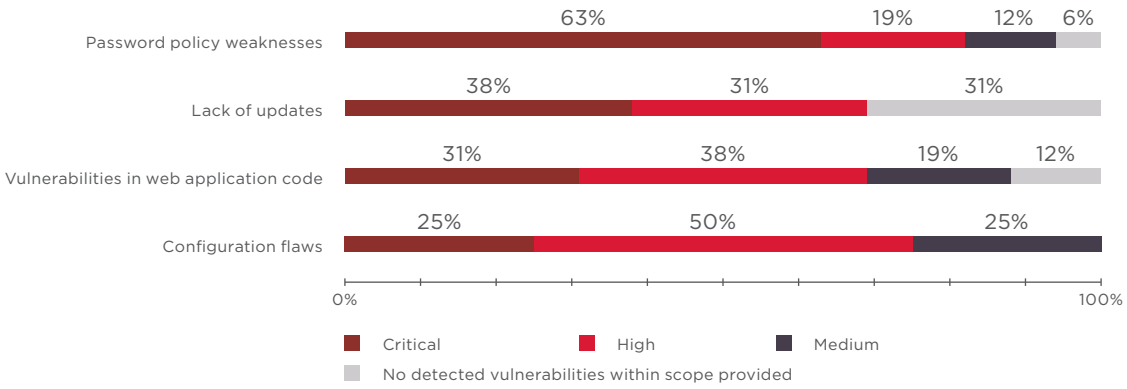

Figure 4. Most dangerous vulnerability found, by category (percentage of systems)

It is worth keeping in mind that penetration testing was performed using the black-box method: therefore, systems may have contained even more vulnerabilities than were detected in our analysis. Client infrastructure could have protection gaps, not reflected in our findings, caused by failure to install updates on time, vulnerabilities in web application code, or use of dictionary passwords. However, the purpose of testing is not to find every single flaw and vulnerability, but instead to provide an objective picture of the state of security against attackers.

External pentesting: results

92%
of companies fell to external pentesters' attempts to obtain LAN access

In 2018, the network perimeter of 92 percent of companies was breached during external pentesting. In one case, access to internal network resources was possible only with the help of social engineering.

In most cases, there were several ways to obtain access to the internal network. Systems had an average number of two vectors each, although for one system there were five separate vectors. At half of companies, the network perimeter could be breached in just one step, usually by exploiting a web application vulnerability.

5 is the largest number of penetration vectors identified at a single company

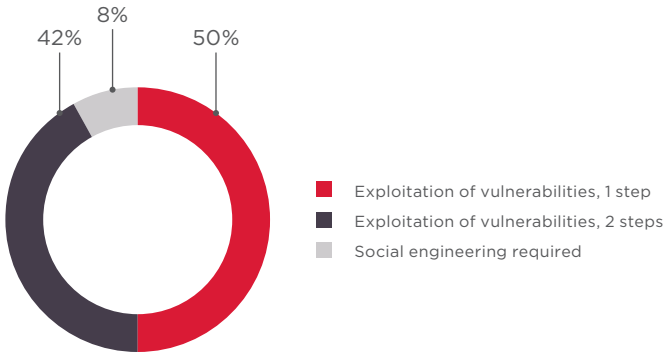

Figure 5. Shortest path to breach network perimeter (percentage of systems)

Three quarters of vectors were caused by poor web application protection, which is the most common issue on the network perimeter. In cases when a vector consisted of multiple steps, a different kind of vulnerability might be used at each step. A typical scenario: bruteforcing of the password of a web application user, followed by exploitation of a vulnerability in web application code, such as the ability to upload arbitrary files to the server.

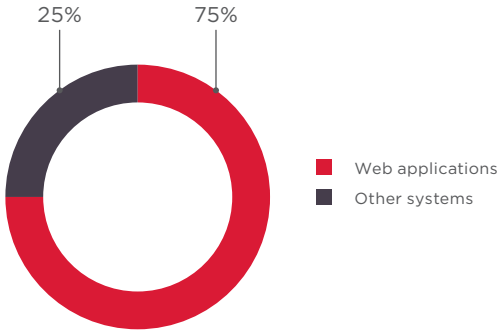

Figure 6. Vectors for penetrating network perimeter

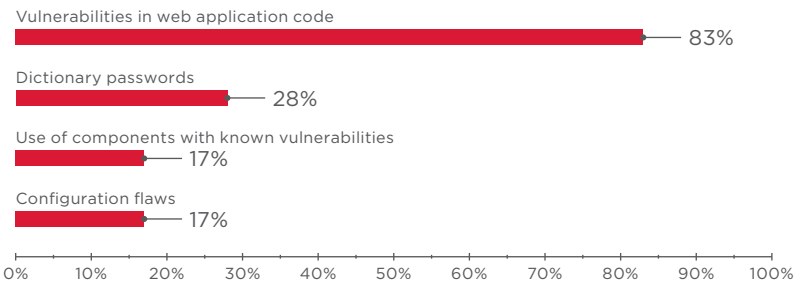

Figure 7. Web application vulnerabilities that allow breaching the network perimeter (percentage of vectors)

Recommendations

Perform security assessment of web applications regularly. As a web application grows in complexity and feature set, the higher the chances of a coding error by developers that allows an attacker to slip through. Such errors are frequently detected during penetration testing, but the best way to find them is white-box testing (analysis of source code). Fixing vulnerabilities usually involves changes to code, potentially requiring large amounts of time. To avoid downtime and disruption, we recommend installing a web application firewall (WAF) to prevent exploitation of vulnerabilities while fixes are pending as well as to protect from new and zero-day vulnerabilities.

Other vectors stemmed from password bruteforcing of Outlook Web App (OWA), VPN servers, and workstations, as well as configuration errors on network equipment. Out-of-date software may contain vulnerabilities enabling control over the server and access to the internal network. Public exploits exist for many such vulnerabilities but demonstrating them is liable to cause disruption, which is why clients generally do not allow doing so during testing.

Exploitation of:

+ Dictionary passwords belonging to users

Penetration testing revealed that access to the OWA service was performed from the domain account test:test1234. The testers connected to OWA and downloaded the Offline Address Book, which lists the domain users. After bruteforcing a dictionary password of one of the users, the testers connected to the Remote Desktop Gateway (RDG) and established an RDP connection with the employee's computer on the internal network.

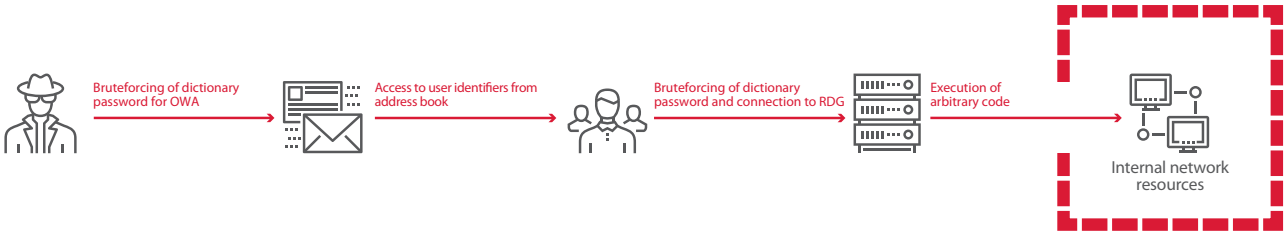

Figure 8. Penetration vector with bruteforcing of dictionary passwords

Exploitation of:

- Interface for hardware management is available to any Internet user
- Dictionary passwords belonging to privileged users
- Use of vulnerable software version—execution of arbitrary code

Many pentest attacks succeed due to the presence of system interfaces on the network perimeter, even when they should be accessible only from the internal network. In recent years, we have repeatedly encountered misconfiguration and vulnerabilities in video surveillance systems, and 2018 was no exception. Testers could watch video from cameras and even run arbitrary code due to old firmware versions. One of the firmware vulnerabilities, CVE-2013-0143, became public five years ago. This just goes to show how important it is to properly delineate the network perimeter and monitor the security status of every system component.

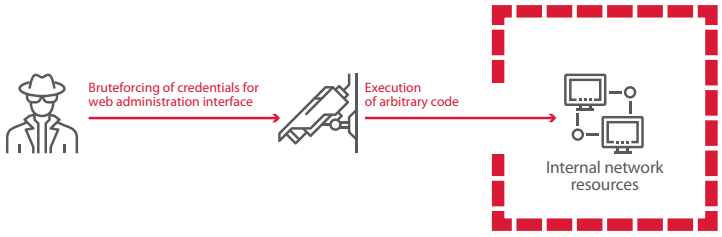

Figure 9. Exploitation of vulnerabilities in video surveillance system

The top 10 vulnerabilities on the network perimeter are essentially constant from year to year. Dictionary passwords had become significantly less common at companies, but rebounded this year back to the top of the list. Use of insecure protocols, including for access to administration interfaces, is also a widespread problem. An attacker can intercept credentials transmitted without encryption and use them to access corporate resources. On more than half of systems, an external attacker could access interfaces for remote access, hardware management, and database management systems.

Recommendations

Minimize the number of services on the network perimeter. Make sure that accessible interfaces truly need to be available to all Internet users. Regularly take an inventory of the resources that are Internet-accessible. Vulnerabilities may appear at any time, since infrastructure configuration is constantly changing. Addition of new hosts, new components, and human error by administrators are all contributing factors.

Forbid use of weak or dictionary passwords. Create and enforce a strict password policy.

19 years
is the age of the oldest vulnerability we found on a system (CVE-1999-0024)

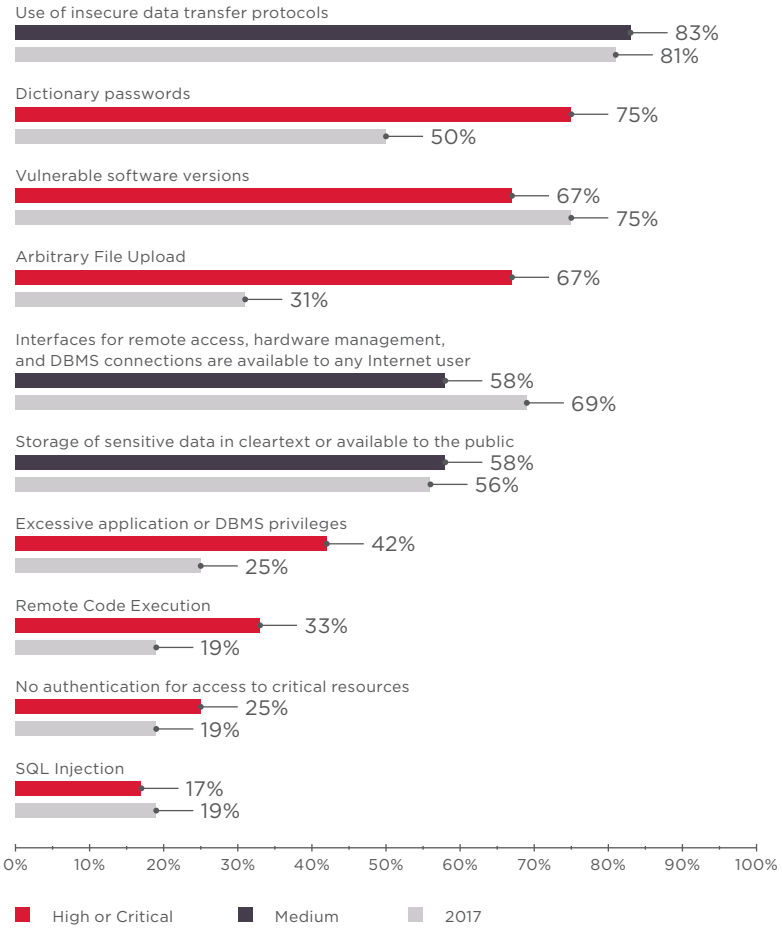

Figure 10. Most common vulnerabilities on the network perimeter (percentage of systems)

Resources on the network perimeter often contain sensitive unencrypted data that could be useful for an attacker: backups of web applications, system configurations, credentials for critical resources, or a list of usernames for which an attacker can bruteforce passwords.

Recommendations

Make sure that sensitive information of potential interest to attackers is not available publicly (such as on web application pages). Such information may include access credentials, corporate address books containing employee email addresses and domain identifiers, and the like. For companies without sufficient in-house capacity for this task, we urge hiring independent penetration testing experts.

Failure to install updates continues to be an issue. This is especially true of applications, web servers, and off-the-shelf web applications.

Exploitation of:

- Use of vulnerable software version—authentication bypass
- Use of vulnerable software version—execution of arbitrary code

During external penetration testing of a client's network perimeter, experts detected an out-of-date version of Cisco TelePresence Video Communication Server. This version is vulnerable to an authentication bypass attack (CVE-2015-0653). As a result, exploitation yielded access to the administration web interface.

The administration web interface contains built-in functionality for downloading updates, which can be used to run commands on the server. The experts created an archive containing a set of shell commands. By uploading the archive to the server as an update file, the testers could run arbitrary commands on the server.

An internal network interface was detected on the server, enabling an attacker to proceed with an attack on the client LAN.

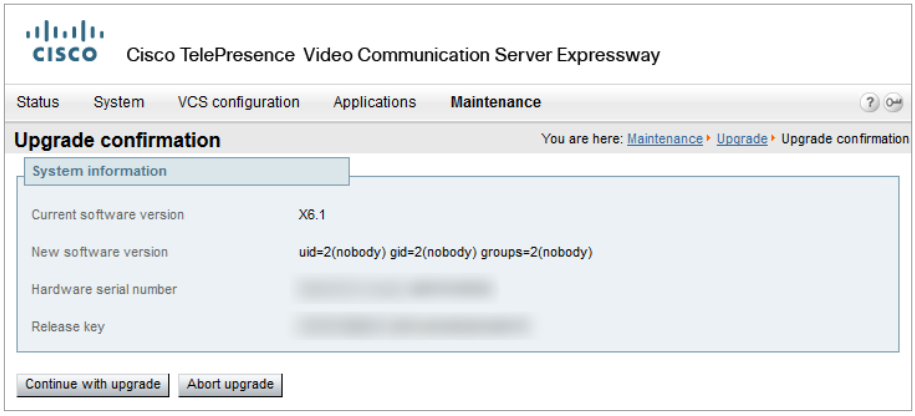

Figure 11. Running the id command shows information about the current server user

Recommendations

Install both OS security updates and application updates in a timely fashion. Make sure that software containing known vulnerabilities does not appear on the network perimeter.

Internal pentesting: results

On 100%
of tested systems, internal pentesting resulted in full control of infrastructure

Full control of internal infrastructure was obtained on all tested systems. On average, doing so required four steps. In one typical vector, dictionary passwords are bruteforced and credentials are recovered from OS memory with the help of special utilities. By repeating these steps, the attacker laterally moves from one host to another, eventually obtaining the credentials of the domain administrator.

Recommendations

Protect infrastructure from attacks aimed at recovering credentials from OS memory. To do so, we urge upgrading all workstations of privileged users, as well as all hosts accessed with privileged credentials, to Windows 8.1 or later (and in the case of servers, to Windows Server 2012 R2 or later) and placing privileged domain users in the Protected Users group. One option is to use modern versions of Windows 10 on workstations and Windows Server 2016 on servers with support for Remote Credential Guard, which allows isolating and protecting the lsass.exe system process from unauthorized access.

Take additional measures to protected privileged accounts (such as domain administrators). Two-factor authentication is a good practice.

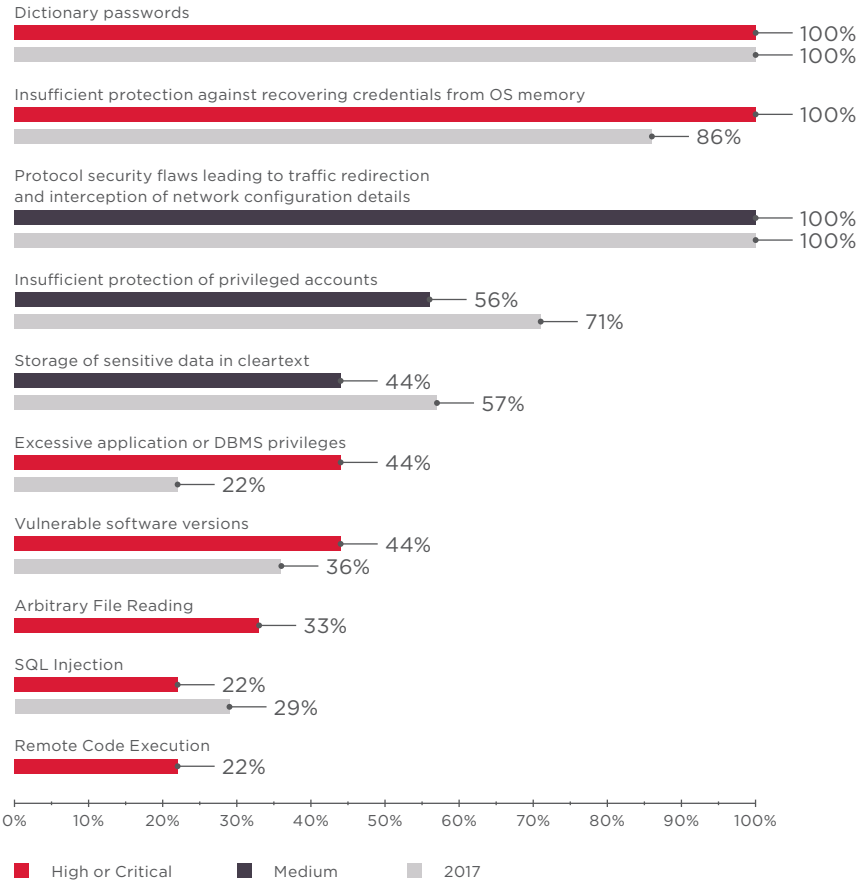

Figure 12. Most common vulnerabilities on the internal network (percentage of systems)

Network traffic analysis was performed at 78 percent of clients. Every network contained flaws that enabled intercepting information transmitted over the network. For instance, 86 percent of tested systems failed to protect the NBNS and LLMNR protocols. Therefore, an attacker can intercept user identifiers and hashes by using NBNS Poisoning and LLMNR Poisoning attacks, and then bruteforcing passwords for the resulting hashes.

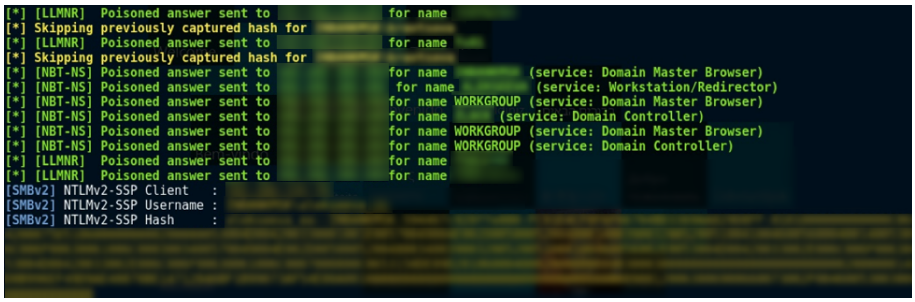

Figure 13. Interception of user credentials via NBNS and LLMNR Poisoning

Recommendations

Whenever possible, disable all Data Link and Network layer protocols on the LAN. If these protocols are needed for particular components, place the components on a separate network segment that cannot be accessed from the user segment.

On internal infrastructure, out-of-date OS versions were the most frequent occurrence, being found on 44 percent of tested systems. Failure to install updates, especially those fixing critical vulnerabilities, enables further developing an attack on the network. On every third system, we found the vulnerability described in security bulletin MS17-010, for which the EternalBlue exploit was made public in 2017. On some hosts, testers were able to escalate privileges using the MS17-018 and CVE-2016-5195 (DirtyCow) vulnerabilities.

Exploitation of:

- Insufficient protection against recovering credentials from OS memory
- Vulnerable software versions— remote code execution (MS17-010)

During internal pentesting, exploitation of vulnerability MS17-010 resulted in access to a server running Windows Server 2012 R2. This version of Windows Server is able to protect account credentials from recovery, but privileged domain users must be placed in the Protected Users group, which had not been done in this particular case. The testers ran mimikatz and thus obtained cleartext usernames and passwords.

One of the passwords belonged to a user with local administrator privileges on Microsoft Hyper-V servers. Since the hard drive of a Hyper-V virtual machine can be copied on the fly, the testers copied the disk of the virtual machine that hosted the domain controller. By obtaining the files ntds.dit and SYSTEM from this copy, and then running secretsdump.py (from the publicly available Impacket kit), they succeeded in extracting the NTLM hashes for domain users, including for the user krbtgt.

```
(.env) > $ ./secretsdump.py Administrator@          -just-dc-user krbtgt
Impacket v0.9.18-dev - Copyright 2002-2018 Core Security Technologies

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
krbtgt:
[*] Cleaning up...
```

Figure 14. Access to hash of krbtgt user password

Possession of the NTLM hash for the krbtgt user allows conducting a Golden Ticket attack. The Kerberos protocol works by providing access tickets to domain infrastructure resources. Privileges for the krbtgt account make it possible to issue Kerberos tickets with any level of access and logging in to resources with maximum privileges. With ticketer.py from Impacket, the testers created a so-called golden ticket, enabling them to run OS commands on the domain controller with maximum privileges.

Eliminating the aftermath of a Kerberos Golden Ticket attack requires not only resetting the password for the krbtgt user twice, but reinstalling all components on the domain infrastructure.

Staff security awareness: results

Social engineering is a classic yet effective way of penetrating a company's internal network. Therefore, in addition to technical penetration testing, it is important to test just how security-conscious employees are. Scenarios, pre-approved by the client, carefully imitate what an attacker might do in a real phishing campaign.

2,639
emails were sent by testers in 2018 as part of security awareness testing

Testers reached out to employees by phone and by email. In phone conversations, they tried to elicit sensitive information from the employee. Emails contained files or web links requesting that the employee enter their username and password. In each case, the employee response, if any, is recorded (link clicked, credentials entered, or attachment run).

Almost one third of employees clicked a link or ran an attachment. One in ten employees entered their credentials in a fake authentication form. A significant number of employees (14%) disclosed sensitive information over the phone or responded to the would-be attacker with additional information about the company: employee names and job titles, work phone numbers, and mobile phone numbers.

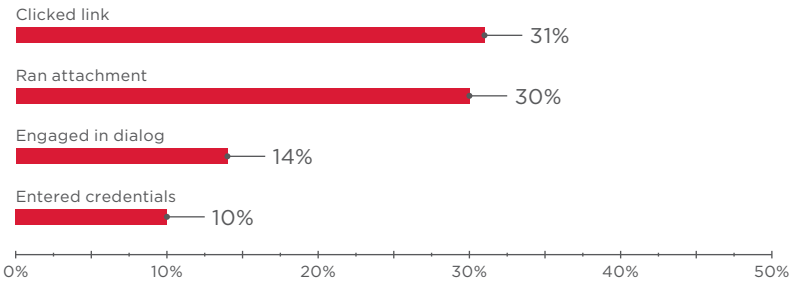

Figure 15. Results of staff awareness testing

Recommendations

To detect and prevent social engineering attacks, we recommend antivirus software with a sandbox for dynamically scanning files and the ability to detect and block malicious email attachments before they are opened by employees. Such antivirus software should simultaneously support solutions from multiple vendors and have the ability to detect signs of hidden or obfuscated malware, as well as block malicious activity across diverse data streams: email, web traffic, network traffic, file storage, and web portals. It is crucial that antivirus software, besides scanning files in real time, automatically perform retrospective analysis of previously scanned files: newer detection signatures may reveal threats in files that had passed scanning in the past.

Regularly train employees to improve their awareness of information security and follow up to verify implementation in practice.

Wi-Fi network testing: results

Wireless networks can serve as a gateway into a company's internal infrastructure. All an attacker needs to do is install free software on a laptop and purchase a cheap modem that supports monitoring of network traffic. Seven out of eight tested Wi-Fi networks were accessible outside of client premises. So with no need to enter the target, an attacker could simply sit somewhere nearby—such as a parking lot or cafe.

Almost all tested networks used the WPA2 protocol with PSK or EAP authentication.

On 5 out of 8
systems, Wi-Fi networks yielded access to the LAN

On 4 out of 8
systems, attacks resulted in maximum privileges on the domain infrastructure

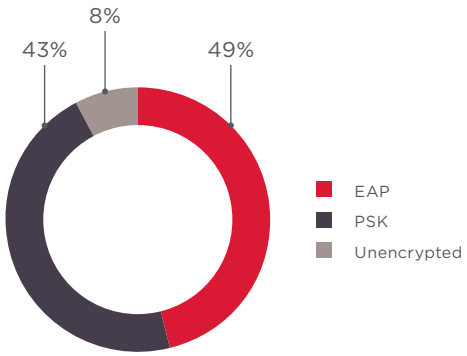

Figure 16. Wi-Fi authentication methods

At one industrial company, it was possible to move laterally from the Wi-Fi network to **ICS equipment**

The choice of attack depends on the authentication method used. For WPA2/PSK, an attacker can intercept the handshake between the access point and legitimate Wi-Fi client, and then bruteforce the password. Stronger passwords are more difficult for an attacker to bruteforce, but our testing showed use of dictionary passwords on half of Wi-Fi networks.

Another attack method—access point spoofing—works regardless of authentication method. If certificate pinning is not used, an attacker can create a fake Wi-Fi access point with the same name (ESSID) as the real access point, but with a more powerful signal. When a client connects to the fake access point, the attacker gets the client's ID and NetNTLM v1 challenge/response value in cleartext, which is sufficient for bruteforcing the password.

Certificate pinning was absent on three systems. Even when it is present, an attacker can "borrow" the name of a popular free Wi-Fi network. Although the legitimate network may be encrypted, an unencrypted fake network with the same name will still be connected to automatically without the user's knowledge. Moreover, so-called KARMA attacks are another option. Many user devices send queries to determine if a Wi-Fi network is in a list of saved Wi-Fi networks. An attacker can create fake access points that imitate the network named in the request. These attacks are combined with use of fake authentication forms, which are disguised as sites of the target company. Upon connecting to the network, the user is redirected to a page with (fake) authentication form requesting that the user enter their corporate account credentials. The success or failure of this attack depends on the vigilance of employees.

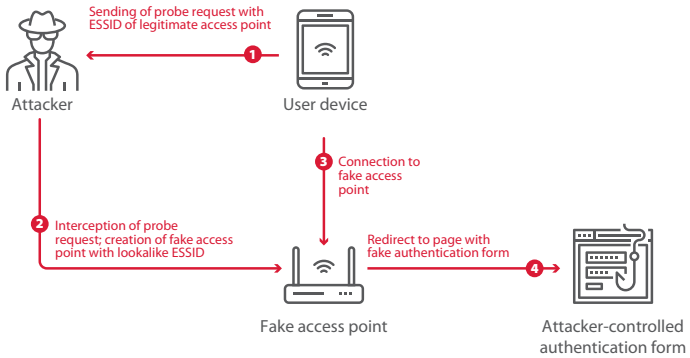

Figure 17. KARMA attack with use of a phishing form

On 7 out of 8
systems, users are not isolated from each other

User isolation is important for guest networks. Company employees should not use such networks from the same devices used to connect to the corporate Wi-Fi network. Otherwise, an attacker with access to an unisolated guest network can attack users to obtain the unencrypted passwords for other Wi-Fi access points to which auto-connection is enabled. As a result, an attacker can obtain the password for a corporate network without even having to attack it directly.

Recommendations

Use strong WPA2 encryption to improve the security of guest networks. Isolate users of the guest Wi-Fi network and do not allow employees to connect to it. The guest network must be separated from the LAN.

The corporate network should be protected with a strong password. Restrict the Wi-Fi signal so that the network is not accessible from public areas. Certificate pinning should be enabled on employee devices to prevent man-in-the-middle attacks with fake access points.

Educate employees on how to safely use Wi-Fi networks. Hold periodic training sessions and verify the results in practice.

Perform regular assessment of Wi-Fi network security in order to identify configuration errors and potential vectors for access to internal networks.

Dictionary passwords: still a problem

Dictionary passwords were found most often with domain accounts and accounts for accessing web applications, both on the network perimeter and on internal infrastructure.

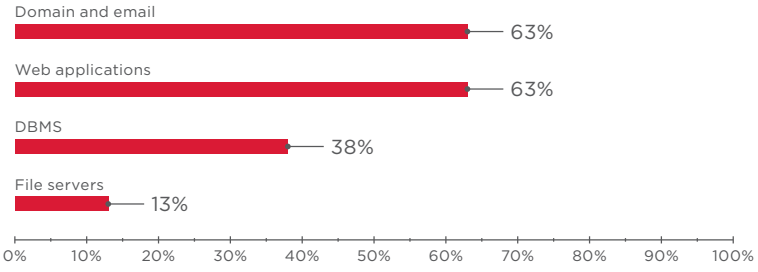

Figure 18. Dictionary passwords used for access to various resources (percentage of systems)

Qwerty123
and similar keyboard combinations remain the most common passwords

admin
is the most popular password among privileged users

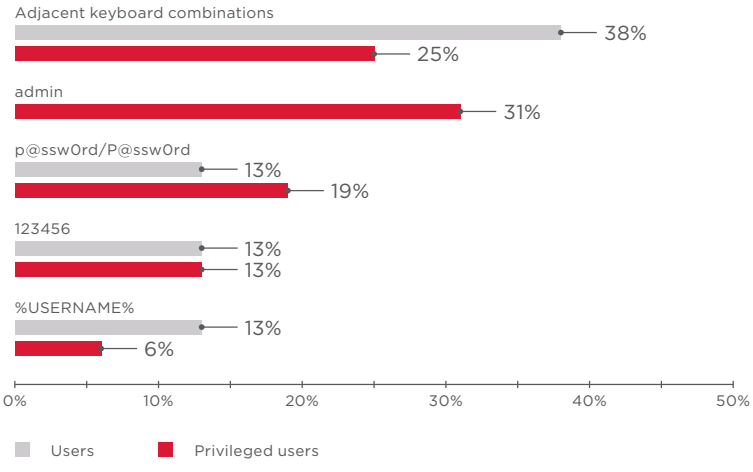

Figure 19. Most common passwords (percentage of systems)

Such weak passwords are often set by default, such as for initial login, until the user sets a stronger one. But sometimes users forget to do so or simply choose "convenient" combinations of adjacent keys, falsely believing that such passwords are sufficiently secure.

Conclusion

Corporate information systems remain vulnerable. Every year, the percentage of corporate local networks susceptible to the actions of an external attacker is increasing. And social engineering and Wi-Fi networks tilt the odds further still in favor of attackers. Both last year and this year, testers were able to take full control over infrastructure at every single client tested during internal pentesting.

Attack vectors usually involve exploitation of known flaws and vulnerabilities, without requiring any great technical skill. Following the security basics is enough to stay relatively well protected. Recommendations for fixing common vulnerabilities are outlined in the relevant sections of this report.

On the network perimeter, the main issue is poor web application security. We advise regularly testing the security of web applications, preferably with white-box testing of source code. As a preventive measure, we also recommend using a web application firewall to prevent exploitation of emergent vulnerabilities caused by code changes or new functionality.

Timely detection is the key to preventing damage and neutralizing threats. Solutions for effective incident response include security information and event management (SIEM) systems, which pinpoint malicious network activity, hack attempts, and attacker presence.

Pentester activity rarely raises the suspicions of corporate information security departments. Actual attackers, therefore, could burrow into infrastructure and stay unnoticed for extended periods. So protection of the network perimeter should be complemented with periodic retrospective analysis of the network to detect any previously unnoticed incidents. Indicators of compromise can be picked up by special solutions for deep analysis of network traffic to detect advanced persistent threats in real time and from saved traffic. These capabilities enable detecting when a hack has occurred and when a network attack is underway, such as use of malicious tools, exploitation of vulnerabilities, and attacks on domain controllers. By reducing the time that attackers are able to remain hidden, companies can minimize the risk of data leaks, ensure uninterrupted operation, and reduce financial losses.

Results confirm that employees tend to have poor awareness of information security issues. Training, with periodic follow-up, is a must. We also recommend antivirus software that scans files in an isolated sandbox, flags malware, and helps to block malicious activity.

For security efforts to pay off, companies must employ an across-the-board approach. Even one or two gaps in an otherwise strong security stance can be enough to allow infrastructure hacks and compromise of critical resources. We strongly recommend penetration testing on a regular basis to identify attack vectors and evaluate the effectiveness of protection in practice.

ptsecurity.com
info@ptsecurity.com

Corp-Vulnerabilities-2019_A4.ENG.0002.04