

Organizational Security Threats and Vulnerabilities

Kimberly Badia

Colorado State University Global

ITS425: Ethical Hacking and Penetration Testing

Dr. Ryan Averbeck

July 4, 2021

Table of Contents

Section 1:
Vulnerabilities and
Threats

3

Section 2:
Prevention &
Countermeasures

11

Conclusion

16

Network Diagram

17

References

18

Section 1

Vulnerabilities and
Threats

What threats are new this year and which have become more prevalent?

- Cloud Vulnerability and Misconfiguration
- Artificial Intelligence Cyberthreats & Fuzzing
- Machine Learning Poisoning
- Social Engineering Attacks
- Deepfake



▶ ▶ 🔍 0:10 / 1:26



Figure 1. Adapted from *Fake Obama created using AI video tool* by BBC News, 2017 (<https://www.youtube.com/watch?v=AmUC4m6w1wo>). Copyright 2021 by BBC.

Why are these threats more common and why are they important?

- Less emphasis on security awareness
- Underfunded security teams
- Most leaks & attacks involve inside participation
- Average attacks cost over \$11 million



Figure 2. From *The 2020 Data Breach Investigations Report – a CSO's perspective* by Martin Jartelius, 2020 (<https://www.sciencedirect.com.csuglobal.idm.oclc.org/science/article/pii/S1353485820300799>). Copyright 2020 by Elsevier Ltd.

What threats remain constant from year to year? Why?

- Injection Flaws
- Security Misconfiguration
- Sensitive Data Exposure
- Broken Authentication / Access Control
- Insufficient Logging & Monitoring

Injection			Security Misconfiguration				
Threat Agents	Attack Vectors	Security Weakness	Attack Vectors	Security Weakness	Impacts		
App. Specific	Exploitability: 3	Prevalence: 2	Detectability: 3	Technical: 3	Business ?		
Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services, and all types of users. Injection flaws occur when an attacker can send hostile data to an interpreter.	Injection flaws are very prevalent, particularly in legacy code. Injection vulnerabilities are often found in SQL, LDAP, XPath, or NoSQL queries, OS commands, XML parsers, SMTP headers, expression languages, and ORM queries.	Injection flaws are easy to discover when examining code. Scanners and fuzzers can help attackers find injection flaws.	Injection can result in data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access. Injection can sometimes lead to complete host takeover.	The business impact depends on the needs of the application and data.	Attackers will often attempt to exploit unpatched flaws or access default accounts, unused pages, unprotected files and directories, etc to gain unauthorized access or knowledge of the system.	Security misconfiguration can happen at any level of an application stack, including the network services, platform, web server, application server, database, frameworks, custom code, and pre-installed virtual machines, containers, or storage. Automated scanners are useful for detecting misconfigurations, use of default accounts or configurations, unnecessary services, legacy options, etc.	Such flaws frequently give attackers unauthorized access to some system data or functionality. Occasionally, such flaws result in a complete system compromise. The business impact depends on the protection needs of the application and data.
Sensitive Data Exposure			Broken Authentication				
Threat Agents	Attack Vectors	Security Weakness	Attack Vectors	Security Weakness	Impacts		
App. Specific	Exploitability: 2	Prevalence: 3	Detectability: 2	Technical: 3	Business ?		
Rather than directly attacking crypto, attackers steal keys, execute man-in-the-middle attacks, or steal clear text data off the server, while in transit, or from the user's client, e.g. browser. A manual attack is generally required. Previously retrieved password databases could be brute forced by Graphics Processing Units (GPUs).	Over the last few years, this has been the most common impactful attack. The most common flaw is simply not encrypting sensitive data. When crypto is employed, weak key generation and management, and weak algorithm, protocol and cipher usage is common, particularly for weak password hashing storage techniques. For data in transit, server side weaknesses are mainly easy to detect, but hard for data at rest.	Failure frequently compromises all data that should have been protected. Typically, this information includes sensitive personal information (PII) data such as health records, credentials, personal data, and credit cards, which often require protection as defined by laws or regulations such as the EU GDPR or local privacy laws.	Attackers have access to hundreds of millions of valid username and password combinations for credential stuffing, default administrative account lists, automated brute force, and dictionary attack tools. Session management attacks are well understood, particularly in relation to unexpired session tokens.	The prevalence of broken authentication is widespread due to the design and implementation of most identity and access controls. Session management is the bedrock of authentication and access controls, and is present in all stateful applications. Attackers can detect broken authentication using manual means and exploit them using automated tools with password lists and dictionary attacks.	Attackers have to gain access to only a few accounts, or just one admin account to compromise the system. Depending on the domain of the application, this may allow money laundering, social security fraud, and identity theft, or disclose legally protected highly sensitive information.		
Broken Access Control			Insufficient Logging & Monitoring				
Threat Agents	Attack Vectors	Security Weakness	Attack Vectors	Security Weakness	Impacts		
App. Specific	Exploitability: 2	Prevalence: 2	Detectability: 2	Technical: 3	Business ?		
Exploitation of access control is a core skill of attackers. SAST and DAST tools can detect the absence of access control but cannot verify if it is functional when it is present. Access control is detectable using manual means, or possibly through automation for the absence of access controls in certain frameworks.	Access control weaknesses are common due to the lack of automated detection, and lack of effective functional testing by application developers.	Access control detection is not typically amenable to automated static or dynamic testing. Manual testing is the best way to detect missing or ineffective access control, including HTTP method (GET vs PUT, etc), controller, direct object references, etc.	The technical impact is attackers acting as users or administrators, or users using privileged functions, or creating, accessing, updating or deleting every record.	Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident.	This issue is included in the Top 10 based on an industry survey .	Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploit to nearly 100%.	
				Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected.	One strategy for determining if you have sufficient monitoring is to examine the logs following penetration testing. The testers' actions should be recorded sufficiently to understand what damages they may have inflicted.	In 2016, identifying a breach took an average of 191 days – plenty of time for damage to be inflicted.	

Figure 3. Adapted from OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks by OWASP Foundation, 2017

(file:///B:/klond_000/Downloads/OWASP%20Top%2010-2017%20(en).pdf). Copyright 2021 by OWASP Foundation, Inc..

What threats do you believe will become more critical in the next 12 months? Why?

- Remote Working Means Higher Potential Exposure
- Ransomware Costs are Increasing
- Spear-Phishing Campaigns are More Sophisticated
- Covid-19 Created Pandemic-Related Security Problems
- More People Working Remotely Than Ever Before
- Cryptocurrency Decreases Risk to Cybercriminals

RANSOMWARE, BY THE NUMBERS



Increase in ransomware attacks, fueled by the pandemic: **148%**



Anticipated global ransomware recovery costs by the end of 2021: **\$20 billion**



Average ransom demand in Q4 2020: **\$154,108** (-34% from Q3 2020)



Average days of downtime in Q4 2020: **21 days** (+11% from Q3 2020)



Percentage of ransomware in Q4 that included the threat to leak exfiltrated data: **70%** (+43% from Q3 2020)



How quickly a new Remote Desktop Protocol (RDP) port — one of the top three ransomware attack vectors — is discovered after first connecting to the Internet: **90 seconds**



How many misconfigured RDP ports are open to the Internet: **4.7 million**



Average number of ransomware attacks that have occurred daily since January 1, 2016: **4,000**



Email messages that contain malware (email phishing is also included in the top three ransomware attack vectors): **1 in 3,000**

Figure 4. Adapted from *Ransomware Stats Every Business Needs to Know* by Marsh, 2021 (<https://www.marsh.com/us/insights/research/ransomware-stats-every-business-needs-to-know.html>)
Copyright 2021 by Marsh, LLC.

Has an exploit been released?

- Critical Remote Code Execution(RCE) vulnerability
- Discovered and Published January 2021
- Current patches are easily bypassed
- Potentially exposes millions of corporate email accounts



Figure 5. Adapted from Critical zero-day RCE in Microsoft office 365 awaits third security patch by Adam Bannister, 2021 (<https://portswigger.net/daily-swig/critical-zero-day-rce-in-microsoft-office-365-awaits-third-security-patch>). Copyright 2021 by PortSwigger Ltd.



Figure 6. Adapted from *Corporate espionage is a lot closer than you may think* by Mark Raybin, 2015 (<https://workingcapitalreview.com/2015/11/corporate-espionage-is-a-lot-closer-than-you-may-think/>). Copyright 2021 by Working Capital Review.

What is the likelihood of an exploit?

- Assume Yes.
- Run deep antimalware scans
- Remove any existing malware
- Mandate all passwords be updated
- Verify inactive user accounts are deactivated

How widely used is the software or system?

- Public and Private Uses
- Student Lab Increases Exposure
- Web Servers
- Email Servers
- High Risk of Exposure

Section 2

Prevention and
Countermeasures

Prevention is Key

- Proactive Identification
- Continuous Scanning
- Focus on raising staff security awareness
- Emphasis on cyber hygiene

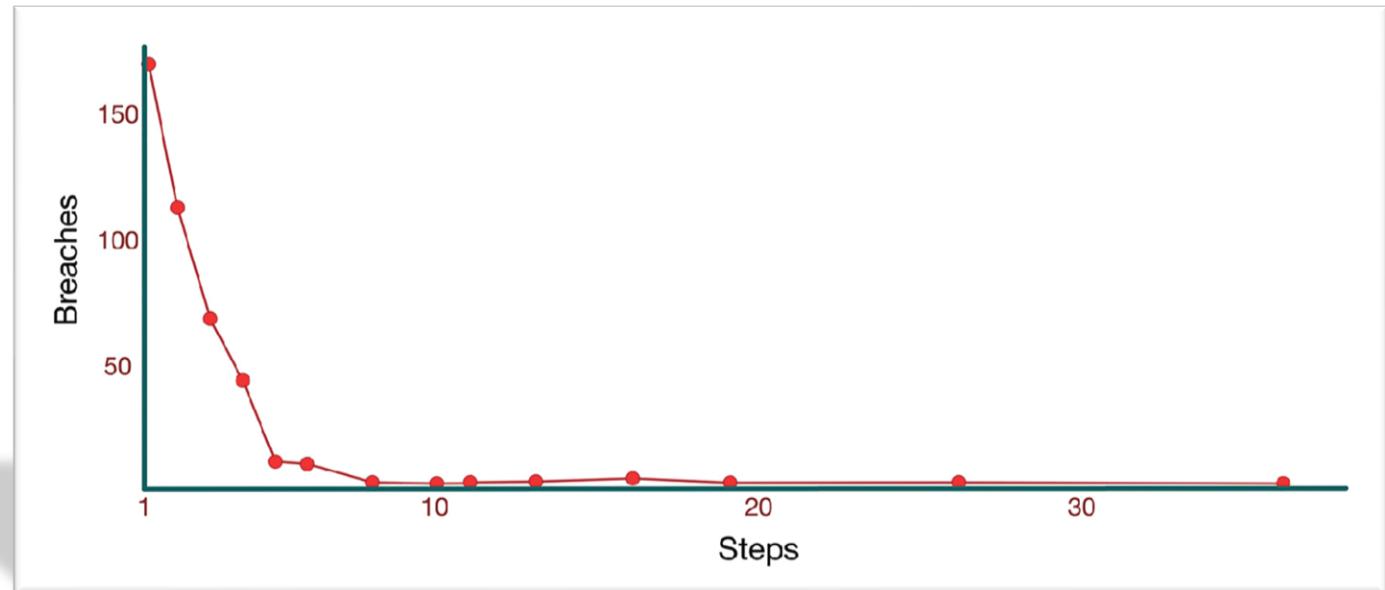


Figure 8. Adapted from *Why Misconfiguration Lead to Breaches - Cloud Security - Risk and Compliance* by Thom Bradley, 2020 (<https://www.nsc42.co.uk/post/cloud-misconfiguration-leads-to-breaches>). Copyright 2020 by NSC42 LTD.

Risk Mitigation

- Access Control – Least Privilege
- Regular system auditing
- Isolated Sensitive Data
- Updated Security Systems
- Active Triage and Remediation Protocols

CISOs see the grenade....

The threat surface includes:

- Targeted 'acts of war' & terrorism
- Indirect criminal activities designed for mass disruption
- Targeted data theft
- Espionage
- 'Hacktivists'



Countermeasure challenges include:

- Outdated security platforms
- Increasing levels of cyber crime
- Limited marketplace skills
- Increased Citizen expectation
- Continuous and ever increasing attack sophistication
- Lack of real-time correlated Cyber Intelligence

Figure 9. Adapted from *Be proactive: Fight and mitigate future attacks with cyber threat hunting* by BankInfoSecurity, 2019 (<https://www.bankinfosecurity.com/be-proactive-fight-mitigate-future-attacks-cyber-threat-hunting-a-12486>).

Copyright 2021 by Information Security Media Group, Corp.

Reducing Vulnerabilities Areas

Up-to-Date Security Systems Strong Password Policies



Figure 10. Adapted from *10 ways to prevent computer security threats from insiders* by David Bianco, 2019 (<https://searchsecurity.techtarget.com/feature/Ten-ways-to-prevent-insider-security-threats>). Copyright 2021 by Tech Target.

Comprehensive, Regular Security Training Risk Assessment



Figure 11. Adapted from *The importance of security awareness training* by S. Digital, 2016 (<https://www.smarttech247.com/news/importance-security-awareness-training/>). Copyright 2021 by SmartTech.

Counteracting an Active Attack: Incident Response

- Identify
 - Assets, Vulnerabilities, Risk Tolerance & Management
- Protect
 - Physical/Remote Access, Maintenance, CIA Triade
- Detect
 - Continuous Monitoring
- Respond
 - During & After the Incident, Mitigation
- Recover
 - System Restoration, Implement Improvements



Figure 12. From *The Five Functions* by NIST, 2021 (<https://www.nist.gov/cyberframework>). Copyright 2021 by National Institute of Standards and Technology, U.S. Department of Commerce.

Conclusion

The rate of cyber attacks is slightly decreasing, but the cost of a breach is skyrocketing – over 15% per annum on average.

New technologies are creating new methods for cybercriminals to attack systems including AI-based attacks to gain access to valuable information.

Addressing how to manage cybersecurity in a world where more people are working remotely than ever is imperative.

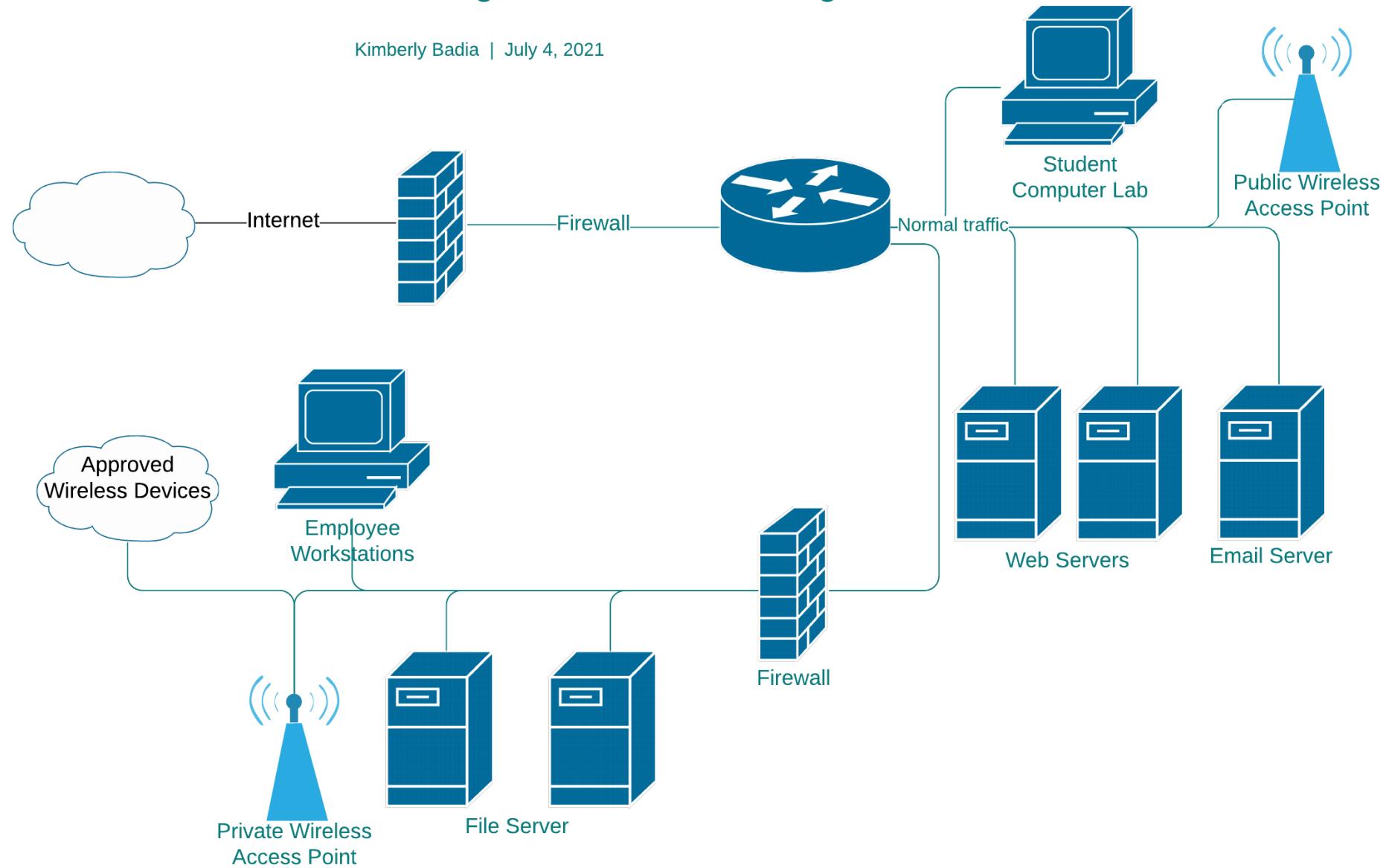
When a vulnerability cannot be eliminated, the risk must be mitigated or transferred when possible. If neither is feasible, additional resources for monitoring must be allocated.

Prevention and proactive vulnerability testing and elimination is infinitely preferable to reactive security measures

Having a comprehensive incident response plan in place prior to a breach can save millions in lost assets, customer and investor faith and prevent fines and penalties from leaked sensitive information.

Adventure Scuba and Diving Institute Network Diagram

Kimberly Badia | July 4, 2021



References

- BankInfoSecurity. (2019, May 15). *Be proactive: Fight and mitigate future attacks with cyber threat hunting.* Bank information security news, training, education. <https://www.bankinfosecurity.com/be-proactive-fight-mitigate-future-attacks-cyber-threat-hunting-a-12486>
- Bannister, A. (2021, January 13). *Critical zero-day RCE in Microsoft office 365 awaits third security patch.* The Daily Swig | Cybersecurity news and views. <https://portswigger.net/daily-swig/critical-zero-day-rce-in-microsoft-office-365-awaits-third-security-patch>
- Belani, G. (2020, January 17). *5 cybersecurity threats to be aware of in 2020.* IEEE Computer Society. <https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020>
- Bradley, T. (2020, October 8). Why Misconfiguration lead to breaches - Cloud security - Risk and compliance. Nsc42. <https://www.nsc42.co.uk/post/cloud-misconfiguration-leads-to-breaches>
- Hoske, M. (2020). Cybersecurity tips: Cybersecurity advice about process, technologies, people (internal) and external threat resulted from the Control Engineering 2020 Cybersecurity Research Report. *Control Engineering*, 67(8), 16.

References

- Jartelius, M. (2020). The 2020 data breach investigations report – a CSO's perspective. *Network Security*, 2020(7), 9-12. [https://doi.org/10.1016/s1353-4858\(20\)30079-9](https://doi.org/10.1016/s1353-4858(20)30079-9)
- Lohrmann, D. (2020, December 11). *2020: The year the COVID-19 crisis brought a cyber pandemic*. Government Technology State & Local Articles - e.Republic. <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html>
- Marsh. (2021, January 22). *Ransomware stats every business needs to know*. Marsh | Global Leader in Insurance Broking and Risk Management. <https://www.marsh.com/us/insights/research/ransomware-stats-every-business-needs-to-know.html>
- NIST. (2020, September 23). *SP 800-53 rev. 5, security and privacy controls for info systems and organizations*. NIST Computer Security Resource Center | CSRC. <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

References

- NIST. (2021, May 12). *Cybersecurity framework: The five functions*. National Institute of Standards and Technology. Retrieved May 24, 2021, from <https://www.nist.gov/cyberframework/online-learning/five-functions>
- Oriyano, S. P., & Solomon, M. G. (2020). *Hacker techniques, tools, and incident handling* (3rd ed.). Jones & Bartlett Learning.
- OWASP Foundation. (2018). *OWASP Top 10 - 2017: The ten most critical web application security risks*. <https://owasp.org/www-project-top-ten/>
- Raybin, M. (2015, November 20). *Corporate espionage is a lot closer than you may think*. Working Capital Review. <https://workingcapitalreview.com/2015/11/corporate-espionage-is-a-lot-closer-than-you-may-think/>