Section 2: Week 5: Propose Strategies and Tools for Cloud Security

Nate Bachmeier

TIM-7030: Managing Risk, Security, and Privacy

July 5, 2020

North Central University

# Propose Strategies and Tools for Cloud Security

NCU Financial (NCU-F) has fallen the victim of targeted malware attacks, and these assaults have disrupted internal systems. For instance, infected workstations are flooding the intranet with bogus traffic slowing communications to a halt. Ransomware has also corrupted several mission-critical systems, such as databases and monitoring solutions, impacting the businesses’ ability to make informed decisions promptly. The organization needs a strategy for restoring the security posture and removing the invasion from its network.

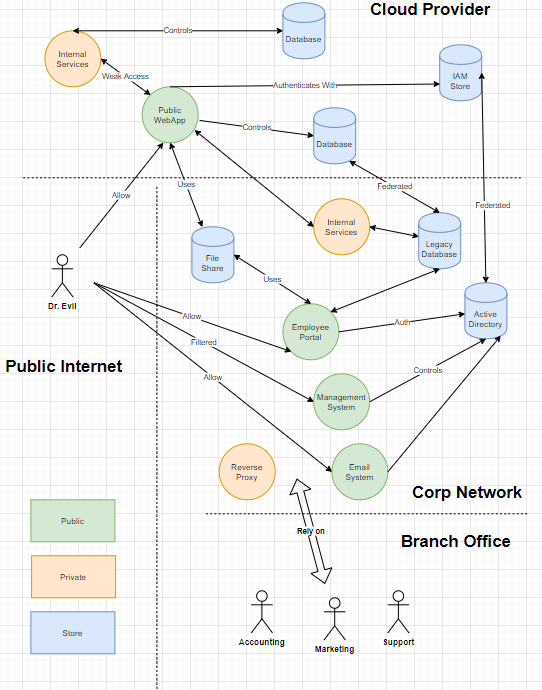
# Section I: Attacking Application Layer

Traditional cybersecurity solutions focus on hardening the network parameter with firewalls and vulnerability scanners. However, this approach is no longer sufficient as attackers center their efforts on the application layer (Astani & Ready, 2016). By design, anonymous users can interact with the organization through public interfaces, such as web services and email. When malicious actors exploit Structured Query Language Injections (SQLi) or embed ransomware into mail attachments—it bypasses these network barriers and allows unauthorized access to information. Further complicating matters, the boundary of the network is becoming more abstract due to the notion of “everything as a service” (Paller, Mahalik, Skoudis, & Ullrich, 2020).

## Poisoning Waterholes

NCU-F has three logical segments to their topology, namely branch offices, the corporate network, and cloud infrastructure (see Figure 1). Supporting business workloads across the company requires high-levels of connectivity between the segments. While possible to limit the exposure through process changes, reduces team velocity, and often encountering political pressure and resistance (Weston, Conklin, & Drobnis, 2018). For instance, a central file server is accessible from the cloud infrastructure via Virtual Private Networking (VPN) and the branch office employees. When the web application becomes compromised, then malware can poison the shared waterhole and burrow further into the network. Elevation paths can also exist across federated stores, such as identity and data management. Perhaps the attacker exploits a vulnerability in the WordPress Content Management System (CMS) and gains access to the associated Postgres database. Sufficient restrictions must exist, or these attacks can cascade through integration points, such as foreign table wrappers, that bridge into related connected systems.

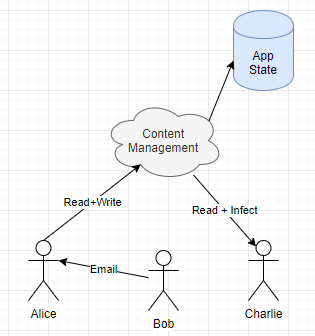
Figure 1: NCU-F Network Topology



## Invalid Encoding Scenarios

Vulnerabilities can exist in the web platform that does not require infrastructural system compromise. Invalid content-encoding can result in command injection at either the presentation (e.g., cross-site scripting) and transport layer (e.g., cross-site response forging). These situations enable the attacker to elevate outside their standard context and bypass security boundaries. For example, Bob sends a malicious link to Alice, which triggers malicious JavaScript code within her web-browsers (see Figure 2). Now the script can use her identity to manipulate the CMS and infect other system users. It can be challenging to prevent these scenarios, given the continuous stream of publically disclosed vulnerabilities in mainstream web platforms.

Figure 2: Cross Content Issues



## Exposed Internal AppState

While there are strategic advantages to manipulating web content and compromising infrastructural components, many attacks do not require either attack vector. Instead, the attacker can focus their efforts on weak controls such as missing authentication and authorization policies. For instance, the session identifier is a numeric counter, stored in a cookie. The user needs to authenticate into the system before getting a valid sequence number but can then fiddle with the value to arbitrarily join other sessions. Other permutations of vulnerabilities exist in query strings, allowing the user to enumerate through the database and find draft content. These drafts might have undisclosed information, like merge announcements or changes to corporate strategy. When the confidentiality of that information is lost, it enables third-parties an upper hand such as buying substantial quantities in that merger target and bidding up the price.

## Economics of Web Attacks

Malicious users seek espionage, sabotage, and subversion tactics against their targets (Kovacs, 2018). These diverse objectives come with varying levels of costs that can ripple across the organization. For instance, the incident can hurt the brand and require public relations experts to control the narrative (Erickson & Neilson, 2018). Lossing confidential information, like intellectual property and internal memos, can reduce its competitiveness, create controversy, and professional embarrassment (Gearan, Rucker, & Phillip, 2016). Many industries might also be liable for negligence, opening the door to litigation and regulatory fines. Small enterprises could easily see total price tags over 5.5 million (Astani & Ready, 2016). More substantial companies can end up paying hundreds of millions while restoring customer confidence (FTC, 2020). Using technologies like ransomware, malicious software that encrypts digital devices, nefarious actors can force an organization to purchase decryption keys before restoring service (Busdicker & Upendra, 2017). Regardless of the recovery strategy, a disruption to the business continuity means a loss in productivity. For Internet-scale applications, like Amazon’s online store, a single minute outage costs over $66K (UpGuard, 2019). Collectively, paying for the cleanup of these different vectors can be impactful to the bottom line and necessitates a proactive design of appropriate controls and system redundancies.

# Section II: Propose an Incident Response

The attack against the NCU-F application interface has enabled international actors to install multiple strains of malware onto the network. The administrative team must devise a response plan to contain the infestation and restore business continuity. While the number of critical issues can be overwhelming, the organization must follow a methodical approach to remediate the situation.

## Corporate Network

This approach must use Identify-Plan-Do-Check feedback loops, which prioritizes assets and objectives that are the most critical first (Radhakrishnan, 2015). Ransomware has corrupt the mission-critical database and payroll department. Without access to that database, NCU-F cannot continue any operations. Meanwhile, the accounting department can temporarily resort to more mechanical processes. After identifying the most critical systems, planning needs to stop the bleeding before drilling into a longer-term solution. For example, deploying the most recent backup of the database, upgrading the software patches, and installing new malware definitions might be an acceptable first step. However, later cleanup will need to revisit configurations and additional access controls.

## Branch Offices

The network administration team will need to quarantine systems that fail to meet specific conditions. One solution is to use System Health Validation (SHV) to confirm the compliance of an endpoint with intranet policies (Microsoft, 2018). These policies can include checks that virus signatures and system patches are recent. A risk exists that the attack could rely on zero-day exploits that can reinfect the machines, though, in practice, this is less likely to occur. Nearly 99% of all malware attacks use public vulnerabilities that are over a year old (Galinec & Steingartner, 2017). This behavior is partially due to reliable zero-day vulnerabilities being worth tens of thousands of dollars on the dark web, versus public exploits are often free (Emery, 2017). However, nation-states and other well-financed actors might have economic means for using such a weapon.

## Cloud Technologies

NCU-F uses VPN technologies for extending the corporate network into the cloud infrastructure (see Figure 1). Operating a hybrid cloud creates many efficiencies but can introduce single points of failure. For example, during the malware attack, the public web application is offline due to dependencies on private datacenter systems. Instead, replication technologies could maintain copies of those private resources within the cloud, constraining the blast radius to the intranet’s edge. The company should also consider the inclusion of anti-malware technologies at various strategic points in the topology. For example, incoming files for the public web application need to stage the content for static and dynamic analysis through tools like ClamAV and Cuckoo (Kilgallon, De La Rosa, & Cavazos, 2017).

## People

One of the byproducts of modern networks having abstract borders is that the rampant malware does not stop at devices owned exclusively by NCU-F. Instead, it continues onto personal devices, which triggers automated backup systems and social media services to further propagating across friends and family members (Balupari & Singh, 2017). At a minimum, the organization has an ethical obligation to guide team members and provide antivirus licenses.

# Section III: Challenges with Wireless Networking