SECURE BEHAVIORS FOR THE HUMAN SUPPLY CHAIN

BRAD GREEN, *Tomball*
Presales Engineer | Arctic Wolf Networks

State Bar of Texas
40TH ANNUAL
ADVANCED REAL ESTATE LAW
July 12-14, 2018
San Antonio

CHAPTER 28

TABLE OF CONTENTS

SECURE BEHAVIORS FOR THE HUMAN SUPPLY CHAIN

I. INTRODUCTION

This intent of this article is to provide a high-level understanding of the common human elements and considerations of cyberattacks. The paper will conclude with a recommenced set of cyber-conscious behaviors to adopt at an individual level in both personal and professional settings. These behaviors are meant to complement the security policies, procedures, and controls in place at your firms.

II. AN OVERVIEW OF CYBERATTACKS AND THREAT ACTORS

Cyberattacks and other types of computer crime are part of the digital world in which we live. Year after year, breaches at organizations both public and private are discovered and disclosed. Both offensive and defensive tools and practices have matured over time in a sort of arms race. Regulations have been introduced and iterated upon in an effort to drive organizations to take reasonable precautions the protect the data of their customers, clients, patients, students, and partners.

Depending on the organizational structure, motive, and maturity of the threat actors, various tactics and techniques may be employed to carry out a cyberattack. MITRE's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK) (https://attack.mitre.org/wiki/Main_Page) contains an extensive knowledge base of adversarial behavior across various stages of an attack. In the planning stage of an advanced attack, the threat actors may expend resources and time identifying and selecting targets, gathering information and identifying weaknesses of the targets in question, and even developing personas (personal and/or organizational identities) designed to facilitate interactions likely to advance the attack stage or reach an operational objective.

III. THE HUMAN ELEMENTS

It is important to remember that cyberattacks, as technologically advanced as they may be, are foundationally human endeavors. Threat actors, defenders, victims, and vectors are ultimately individuals or groups of individuals with strengths, weaknesses, and limits of knowledge, though they may vary greatly in organizational size, structure, and access to resources.

Threat actors are individuals or groups who carry out offensive operations. They can be generally described as one of four types of actor, each of which has a broad threat gradient based on capabilities, organization, motive, and resources. Cybercriminals are generally financially motivated and may range from individuals perpetuating petty crimes to large criminal organizations carrying out sophisticated heists. Hacktivists have motives to achieve political or social change. Insider threat actors range from well-meaning workers unaware that they are carrying out their functions in an insecure manner to malicious insiders determined to cause harm to their organization and/or profit in some way from their actions. State-level actors are another category entirely, but one that private organizations may find themselves targeted by for various reasons depending on their operations.

The defenders responsible for securing organizations consist of employees and/or third-party contractors. The number and focus of defenders as well as their allocated resources depends on an organization's size and risk models. This can range from a fully outsourced security function to a small subset of the IT department to a formal organizational structure within the business. Even in larger organizations.

Other individuals involved in a cyberattack may be vectors, victims or both. Victims are those who suffer the repercussions of an attack while Vectors are individuals who are somehow (wittingly, willingly, or neither) instrumental to the attack. The CEO of a small business who has their email account compromised and used to convince an unsuspecting and well-meaning employee to initiate a fraudulent wire transfer would be a good example of both. At the core of this type of email-initiated wire transfer fraud, the relationship between the CEO and the Employee was leveraged to illicit the desired action.

IV. THE HUMAN SUPPLY CHAIN

The National Institute of Standards and Technology (NIST) recently updated their Framework for Improving Critical Infrastructure Cybersecurity (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf). This new version includes updates to recommendations on managing cybersecurity risk through an organization's business and technology suppliers and buyers. Interactions between humans could be thought of as an analogous supply chain, where the interactions between individuals may carry risk implications related to a cyberattack to upstream or downstream parties.

A. "Upstream" and "Downstream" considerations of legal interactions

The trusted relationship between attorney and client is one that has potential to be abused by threat actors in various ways. Each party has access to information about the other that an attacker may value, and it is expected that calls to action between the parties are often carried out - clients will open the documents or click the links you send them and vice-versa. Security controls should be in place on both sides of the relationship, and organizations are increasingly requiring evidence that a security strategy is in place and

viable. Cybersecurity awareness training for an organization's workforce is often a component of the overall risk management strategy. The purpose of awareness training is to instill behaviors that mitigate attacker techniques related to human vectors.

B. Weaknesses of the Human Vector

Humans are remarkably predictable creatures, though as individuals we often consider ourselves immune from the very types of manipulation that have been shown by advertisers to work so well. We have patterns of behavior that we develop and reinforce over time. Changing behaviors, especially longstanding ones, is difficult (as anyone who has ever attempted a new diet or workout regimen is well-aware). Bad security habits or underdeveloped good habits have real risk implications to an organization, and the human attack vector is arguably the most difficult to secure.

Part of this difficulty lies in the sheer volume of information that is available about an individual. Between volunteered information on social networks, information in the public domain, and information exposed in the litany of data breaches over the years, attackers have a wealth of data available to gather about an individual or environment before even making contact. This is referred to as Open-Source Intelligence Gathering, or OSINT for short.

Social Engineering is the practical application of behavioral science as a means to illicit a desired response or action. In the context of a cyberattack, it can be thought of as exploiting weaknesses in the human attack vector to meet an operational objective such as acquiring information, gaining access, or otherwise advancing the stage of an attack. A skilled social engineer armed with the right information can accomplish surprising things. One does not have to be a Frank Abagnale (a confidence trickster famously portrayed by Leonardo DiCaprio in "Catch Me if You Can") or Kevin Mitnick (self-proclaimed "The World's Most Famous Hacker") to get an unsuspecting target to open an attachment, click a link, or share information.

V. SECURE BEHAVIORS

What follows are some general recommendations for behaviors meant to increase security posture at an individual level. If the vast majority (or all) of the recommendations laid out in this section are familiar, please consider them encouragement. Improvements to these basic behaviors can assist defenders in their efforts to protect you, your clients, and your organizations.

A. Email

i. Why it matters

Email remains a common attack vector and an organization's email contains a treasure trove of data. Phishing emails are relatively easy to craft and deliver to a broad audience with a predictable rate of success. Spear-phishing or "whaling" involves detailed information gathering on a high value target and carefully crafting scenarios to illicit a desired response or action. These scenarios may be composed of a sequence of one or more emails, phone calls, text messages, social media posts/messages, or other personal interactions, and are used to advance the stage or otherwise meet an operational objective of an attack.

ii. What to do

Examine the content of emails from unrecognized senders, and the content and context of emails from recognized senders. Consider validating instructions for emails implying urgency and/or unusual behavior from trusted senders, especially as related to the interaction with untrusted documents or links and calls to action around financial transactions. Beware of unsolicited or unexpected emails prompting you to log in to a service or reset your password, especially if you do not recognize the service in question. Never click a password reset link if you did not initiate the reset request. Do not follow links or open attachments from untrusted sources. Be an early warning system for your firm by alerting the security team if an email seems phishy. Even if you fell for it. The sooner the better.

B. Passwords and Strong Authentication

i. Why it matters

From a defender's perspective, authenticated user sessions are a tricky control point. Users must be enabled to perform the tasks necessary for their work, and they leverage an ever-increasing number of tools and technologies to perform those tasks. Organizations may have implemented some sort of access brokerage, single sign-on, or other forms of authentication federation to reduce the number of passwords that must be managed by users, though the number of passwords a user has is still surprisingly high.

Password complexity and rotation rules vary account to account, and the large number of passwords users are forced to manage generally cause users to adopt insecure password behaviors. These behaviors include easily-guessed passwords, passcodes, and password patterns, reusing passwords across multiple accounts, and storing written passwords in easily accessed locations like the side of the monitor or under the keyboard.

ii. What to do

Never reuse passwords. Create strong unique passwords by increasing length and/or complexity and avoid using guessable or predictable patterns that can fall to simple word-mangling routines (eg. P@ssw0rd1). Consider using passphrases (a series of words in an easily remembered sequence) where possible. Be aware that poorly crafted passphrases and patterns can still be easy for an attacker to guess or brute-force. Passwords

and passphrases, no matter how long or complex, are often not good enough on their own.

Multi-factor authentication should be leveraged wherever possible. This is the use of more than one authentication factor consisting of something you know (password/passphrase), something you have (one-time code on mobile device or physical authentication token), or something you are (fingerprints or other biometric data). While each one of these factors has weaknesses that can be defeated by a well-resourced and determined attacker, their combined use makes the authentication system more robust. https://haveibeenpwned.com/ enables you to see if your email address is used as an account name across a large number of sites that have had a breach where passwords were exposed. A relatively new feature of the site will also let you check if a password exists in their dictionary of over 500 million passwords. Change any and all exposed passwords immediately anywhere they have been used and avoid similarity in the new passwords or passphrases.

The use of password managers or vaults are an effective way to enable the creation and use of unique passwords that meet the varying complexity requirements for each account while only having to remember a single (very strong!) master password or passphrase. Such tools may also have advanced features such as notification of passwords which are old, reused, or exposed in a data breach. Other features such as the automation of password changes and integration with other authentication factors can make strong authentication practices more palatable for everyday use.

C. Account Privileges

i. Why it matters

In the event an account is compromised, the attacker may operate under that account's context for as long as they remain undiscovered. They are able to access all data available to that account and write or execute data or applications under the guise of the account. The implications of this are varied, but good examples to consider would be the context of email or shared file access. An attacker who has compromised a user's credentials or gained access to a user session can read any data stored locally or on network resources that the compromised user can access. They may also execute the functions of any installed application (eg. send emails, share documents, etc.) If the account is privileged, they can also install additional applications or services and extract cached credentials.

ii. What to do

Apply principles of least privilege wherever possible. Use an unprivileged context for normal operations and only log in to systems under an administrative context when necessary. Use strong authentication (strong, unique passwords at a minimum, multi-factor authentication where possible) for administrative access.

D. Public Networks / Guest Wi-Fi

i. Why it matters

Open wi-fi networks can be accessed by anyone, and the security of these networks is often unknown. If the network is not properly segmented, an attacker may be able to scan other connected devices for potentially exploitable vulnerabilities. It is also possible for attackers in close proximity to spoof known SSIDs and trick your device in to connecting to an access point they control. This type of man-in-the-middle attack enables the attacker to see all network traffic being transmitted from your device. If that traffic is not properly encrypted, an attacker may be able to gain access to information within the data streams including documents, emails, passwords, cookies (which may be able to be replayed to spoof authenticated sessions with a web service), etc.

ii. What to do

Avoid using untrusted wireless networks. If you do connect to an untrusted network, ensure your operating system, applications, and security software are up to date with the latest security patches prior to connecting and immediately open a VPN connection to encrypt your traffic. Be sure to regularly forget previously-joined networks as devices beacon the SSID of networks they know about, providing a potential man-in-the-middle attack vector to an attacker in close proximity.

E. Devices – Work AND Personal

i. Why it matters

Physical access to a device bypasses several defensive controls and may allow an attacker access to locally stored data. Locally installed applications and configurations may grant the attacker additional entry vectors into trusted networks. If the attacker obtains root or SYSTEM level access it is possible to extract cached credentials to other accounts that have authenticated to the device, which may be used to move laterally through the network and/or gain access to additional resources.

ii. What to do

Security updates and patches should be regularly applied to all operating systems and applications. Only install licensed applications from trusted developers and delivered via trusted mechanisms. Do not root or jailbreak mobile devices. Laptops and mobile devices should be encrypted to mitigate the risk of a lost or stolen device (this may be as simple as setting a strong passcode on mobile devices). Host-based firewalls (often included as part of the OS) should be turned on and security software installed and kept up-to-date. Do not leave mobile devices or laptops unattended in

untrusted environments, and always lock the screen when the device is not in use.

F. Data Access, Storage, and Transfer

i. Why it matters

Attackers may have several objectives regarding data ranging from its theft to denial (eg. Ransomware). Proper precautions should be taken with regards to the handling of confidential data to prevent unauthorized access. These precautions should be a combination of technology controls and good data handling practices by those with access.

ii. What to do

Be aware of your surroundings and the contents of the data you are accessing. Remember that there's a camera on every phone these days. Use a privacy screen if you will be accessing sensitive data in public areas. Use only trusted devices and mechanisms to access, share, and store data. Maintain backups to ensure the availability of data and secure those backups to ensure the confidentiality and integrity of said data.