Innovating the Human Factor

In information security, one of the standard axioms is that people are the weakest link. Trust forms the foundation of society. Though in the last few years, we have seen the consequences of specific breakdowns in that trust. However, trust still drives things. Humans still trust. We humans want to be able to trust. So much breaks down when trust is lost, which is why people are the weakest link.

Predators Prey on Trust

Taking a step away from the world of audit and compliance, think about the various phone scams that have become common. These phone scammers prefer to target older people.[1] They know that the older a person is, the more likely they are to trust what the scammer is saying. The scammers also know that if they are able to successfully scam an older person, then that person is less likely to tell anyone about it. Scammers are predators. They prey on the trust of people, mainly the elderly.

In reality, anyone looking to abuse our systems is a predator. Unless they have a zero-day in hand and a delivery method, these scammers will naturally consider preying on people's trust to succeed. This is true whether we are thinking of an external adversary or an insider threat. Trust, oddly enough, presents opportunity.

What to Do About It?

Finding oneself in a situation where you cannot trust anything or anyone is scary and counterproductive. We have seen situations emerge where trust was lost, such as with East Germany during the Cold War.[2] Increasing awareness when there is a lack of it is important, but care must be taken so that we do not cross the line into paranoia. Generating paranoia is counterproductive. There is a phrase for it: fear, uncertainty and doubt (FUD).

We need new solutions that help people access and utilize resources in a way that is intuitive without breaching trust. Some of these solutions require interaction; some do not. The bottom line, however, is that we need to think of new ways to handle attempts that use our inherent trust against us.

Beyond Trust

Not every issue revolves around trust, however. The human factor also includes human error, whether the result of negligence or not. It involves insiders who have an understanding of a system's weaknesses. They take advantage of said weaknesses for their own gain. The more that humans interact with systems, the more likely it is that there will be issues. So how do we mitigate the human factor? Let us start with the obvious solution: automation.

Automation and Reducing Unnecessary Human Involvement

I write a lot about automation because it has the potential to solve many problems. It frees people from repetitive tasks. It reduces errors. It ensures consistency in processes. It can take advantage of scale. Automation can often finish work faster than a person would.

K. Brian Kelley, CISA, CSPO, MCSE, Security+
Is an author and columnist focusing primarily on Microsoft SQL Server and Windows security. He currently serves as a data architect and an independent infrastructure/security architect concentrating on Active Directory, SQL Server and Windows Server. He has served in a myriad of other positions including senior database administrator, data warehouse architect, web developer, incident response team lead and project manager. Kelley has spoken at 24 Hours of PASS, IT/Dev Connections, SQLConnections, the TechnoSecurity and Forensics Investigation Conference, the IT GRC Forum, SyntaxCon, and at various SQL Saturdays, Code Camps and user groups.

Enjoying this article?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

We know that removing people where we can has the potential to improve performance, but it can also potentially improve security if the correct approach is taken. Case in point: Microsoft ran a data center underwater for two years. Not only did it have a low number of server failures (likely due to the atmosphere), but there were no real concerns about physical security for the data center itself. However, such a solution did require communications through physical cables. Microsoft chose to use post-quantum cryptography to encrypt the traffic along the wire.[3] Microsoft chose the right solution to handle the major issue it was facing: encrypting data in flight.

Again, with automation, anything to do with identity should be automated wherever possible. For instance, when a human resources (HR) representative enters a new record into the HR management system (HRMS), it should initiate the provision of the appropriate user accounts with the relevant security. If a user leaves the organization, that information should also be something that the HRMS platform originates as a deprovision event. Otherwise, we are relying on other methods of coordination to ensure that an account is properly created or disabled and deleted. The more that this process is manual, the more likely that an oversight is going to happen.

Behavioral Analysis

The best way to recognize that something is wrong is to continuously monitor the system when everything is fine. By performing said monitoring and the subsequent analysis, the security system learns what is normal behavior. Some security systems can effectively whitelist certain operations based on its definition of "normal." The system then reports and/or blocks exceptions to that normal behavior. This kind of defense has been around for a number of years, especially with host and network-based intrusion prevention systems.

Recently, I have been seeing it applied to logins, especially for privileged accounts. For instance, if there is never a case for an administrator of an organization to log in from a foreign country, if the system detects the origin of a login request outside of the country, the system automatically blocks the request and alerts the appropriate people in the appropriate manner. This type of protective solution is usually called conditional access. This is an example of an innovation that does not require a user's interaction unless there is an anomaly.

Another example for such a system is with respect to after-hours access. If a certain class of an organization's users should be logging in only during the business day and a login attempt is made outside of those hours, then it can be blocked and reported accordingly. This may mean the difference between an adversary successfully breaching the system and being detected on the way into the system.

> "THE BEST WAY TO RECOGNIZE THAT SOMETHING IS WRONG IS TO CONTINUOUSLY MONITOR THE SYSTEM WHEN EVERYTHING IS FINE."

Alternate Means of Identification

Microsoft has gone on record stating that it wants to get rid of passwords.[4] It is not alone; other major technology vendors say the same thing. The reason is simple: Passwords are relatively easy to compromise. So many passwords have been exposed in data breaches that there are now services to check if a given password is one that has been published online.[5] Previously leaked passwords are at greater risk because adversaries know to try them.

This is why multifactor authentication (MFA) has come to the forefront. Many MFA solutions, however, require a break in workflow. For instance, an authenticator application that I use requires me to get my phone, log in, access the authenticator and find the code that I need to enter into the system. A different authenticator requires a code per identity credential, so not only do I have to go through the steps for the other authentication application, I have the additional code entry requirement. This is why biometrics is touted more and more heavily, whether the application reads your fingerprint on your mobile device or you are logging in via facial recognition on your workstation. It is less cumbersome for the way we operate.

Putting It All Together

When we do not keep up with innovation, we will face some serious trouble due to cyberattacks that exploit the human factor. As a quick case study, let us look at how Colonial Pipeline was breached and infected with ransomware. Mandiant's testimony[6] indicated that:

- An account had a reused password, one known from a data breach.
- The account was inactive or was supposed to be inactive.
- The attack used a legacy virtual private network (VPN) connection to gain access.
- The VPN did not require MFA.

The reused password is a user awareness issue, as the assumption is that the actual user had used the password somewhere else, but it is possible that Colonial Pipeline could have tested for it. The inactive account speaks to a potential automation solution or identifies a weakness in the solution if Colonial Pipeline had one implemented. The fact that the cyberattack used a legacy VPN is not concerning. Although, this may be a case where conditional access could have helped if it was not a legacy product. The bigger concern was that the VPN did not require MFA.

In other words, the reason that Colonial Pipeline went down was not because of some new, novel approach by hackers. Rather, it was because Colonial Pipeline had not kept up with innovations to deal with the human factor.

The Future

Many of today's solutions to mitigate the human factor have their issues. They definitely need tweaking and improving. If you spend time looking at biometric controls, you will see that there are still weaknesses that a creative person will develop as a means to attack or there are issues with implementation. In a classic case demonstrating weaknesses, when fingerprint biometrics first came into use, a group of security researchers tested fingerprint authentication with a simple attack: They threw a ball to a person, retrieved the ball, lifted the fingerprint from the ball, made a "gummy finger" with gelatin to create a fake finger and beat the authentication.[7]

It is likely always going to be an escalation race between adversaries/creative researchers and the ones developing solutions to counter attacks. In addition, outside-of-the-box thinking may result in someone developing an approach no one has thought of to deal with the problem. That is how public-private key cryptography came to be, regardless of what story you know.[8] Dealing with the human factor is going to take innovation for the foreseeable future.

> "IT IS LIKELY ALWAYS GOING TO BE AN ESCALATION RACE BETWEEN ADVERSARIES/CREATIVE RESEARCHERS AND THE ONES DEVELOPING SOLUTIONS TO COUNTER ATTACKS."

Endnotes

1 Fair, L.; "Scams and Older Consumers: Looking at the Data," Federal Trade Commission Consumer Information, USA, 23 October 2019, *https://www.consumer.ftc.gov/blog/2019/10/scams-and-older-consumers-looking-data*

2 Oltermann, P.; "Enemies Everywhere: Photos Show the Absurdity of Life Under the Stasi," *The Guardian,* 20 March 2020, *https://www.theguardian.com/world/2020/mar/20/enemies-everywhere-photos-show-absurdity-life-under-stasi-east-germany*

3 Judge, P.; "Project Natick: Microsoft's Underwater Voyage of Discovery," Data Centre Dynamics, 5 January 2021, *https://www.datacenterdynamics.com/en/analysis/project-natick-microsofts-underwater-voyage-discovery/*

4 Hanson, M.; "Microsoft Aims to Kill Off Passwords in 2021," *TechRadar*, 18 December 2020, *https://www.techradar.com/news/microsoft-aims-to-kill-off-passwords-in-2021*

5 haveibeenpwned.com, pwned passwords service, *https://haveibeenpwned.com/Passwords*

6 Culafi, A.; "Mandiant: Compromised Colonial Pipeline Password Was Reused," *TechTarget* Search Security, 9 June 2021, *https://searchsecurity.techtarget.com/news/252502216/Mandiant-Compromised-Colonial-Pipeline-password-was-reused*

7 Matsumoto, T.; H. Matsumotu; K. Yamada; S. Hoshino; "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," Proceedings of SPIE, vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 24–25 January 2002, *https://www.cryptome.org/gummy.htm*

8 Levy, S.; "The Open Secret," *Wired*, 1 April 1999, *https://www.wired.com/1999/04/crypto/*