MultiFactor Authentication

Ask anyone worth their salt in security and they will tell you passwords are becoming a thing of the past, or rather already have. The number of data breaches grow each year, and yet weak passwords and password policies still remains an issue for security everywhere. According to the Verizon Data Breach Investigation Report, 81% of confirmed data breaches involve weak, default, or stolen passwords, with at least 59% of users reusing these compromised passwords for other systems, or in some cases the same. (a)

In the 1980's the answer seemed to two-factor authentication when Security Dynamics Technologies patented a method for identifying an individual, the technology for which was later patented by AT&T in 1995 (b). For a while, in the beginning, the idea of carrying around a hard token was not well received, then along came the smartphone, simplifying two-factor authentication for everyone by having the means for two-factor authentication right in their pockets. As we adapt, so must our adversary & evidence, such as the Reddit hack of 2018, has shown that using hard tokens, SMS and even biometrics may not be enough anymore. Hackers are discovering techniques to circumvent two-factor authentication by using mobile device malware, SIM card swap, or access through SS7. (c)

So, where do we go from here? Enter the next generation of multifactor authentication (MFA), something several companies are working diligently to bring us in 2019 to help enhance your company's culture of zero tolerance security. With the emergence of Blockchain, enhancements in mobile authentication and machine learning we continue to move forward.

Blockchain

Blockchain offers authentication in such a way that encrypts and stores data so it removes single points of failure, such as having servers where login information might be stored. With this technology a public key in stored in the blockchain, while the private key is stored on the user's device. This can be combined with biometrics to provide even stronger security, instead of using just passwords.

Combine the blockchain technology with that of single sign-on, which allows users to verify their identity only once and then access multiple services across the corporate network. However, it should be mentioned that using single sign-on with passwords alone can be even more dangerous than not having single sign-on. This is due to the fact that if the passwords are compromised the attacker would have access to those same multiple services.

Mobile Authentication Platform

Two factor authentication via short message service (SMS), more commonly referred to as text messages, is being deemed less secure as time goes on, almost even end of life. Driven by instances like Facebook users when they started receiving spam messages due to a two-factor authentication system bug, developers are pushing forward to help create authentication that is practical for both individuals and enterprise.

In 2017 a task force was formed by Verizon, T-Mobile, Sprint & AT&T called the Mobile Authentication Task Force (d). In September of 2018 they unveiled Project Verify, their mobile authentication platform to help strengthen and simplify authentication for both consumers and businesses. The new mobile authentication platform will allow systems to authenticate users based on several factors including; IP address, SIM card registered, phone model, and location.

Essentially, this platform, and others like it, will be reducing risk by analyzing the data and activity on the mobile network to determine a user's identity.

Artificial Intelligence & Machine Learning

Looking forward, with AI becoming more prevalent throughout the infosec industry, it is now being leveraged to increase the security within authentication. The machine learning can help identify users based on several different factors; log-in times, devices used, browsers used, resources the user typically accesses, and even clicking or typing habits.

Should any behavior deviate from the baseline that has been established the system reacts and requires the user to complete authentication challenges, which can even include proving ownership of the device, biometric verification, or getting approval from a network or security administrator.

This is commonly referred to as risk-based authentication, which allows companies to increase the level of difficulty of authentication only when a threat is detected. In addition to the machine learning, the risk-based authentication can determine if a user is who they say they are based off geographic location, status and type of antivirus updates, jailbreak or root detection (for mobile), OS version and even whether the connection is coming from a proxy or a legitimate system. This approach to authentication allows your infosec program to grow with your organization & help prevent credential attacks by automating access policies based on behavior.

Conclusion

SecureNation understands that moving to machine learning and behavior analysis are steps that can be seen as a pricey move. However, by implementing a program that can automate policies with individual risk scores, detect early signs of breaches w/ behavior analytics, and prioritize the issues that are most critical, you can free up your team to pay attention to what matters most to your organization. Need demo's lined up for your next project? Let SecureNation free up your time with vetting and negotiations, because managing the cyber security program you already have is more than enough work. Ask us today how we can save you valuable time & effort in your procurement process.

> *"Let SecureNation free up your time with vetting and negotiations, because managing the cyber security program you already have is more than enough work."*

References

(a)Verizon Enterprise (2018). 2018 Data Breach Investigations Report. [online] Verizon Enterprise. Available at: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf [Accessed 23 Apr. 2019].

(b) Huang, S. (2019). Two-factor-authentication For Your Token. [online] Medium. Available at: https://medium.com/coinmonks/two-factor-authentication-for-your-token-6f1e51b793a8 [Accessed 23 Apr. 2019].

(c)Townsend, K. (2018). Attackers Circumvent Two Factor Authentication Protections to Hack Reddit | SecurityWeek.Com. [online] Securityweek.com. Available at: https://www.securityweek.com/attackers-circumvent-two-factor-authentication-protections-hack-reddit [Accessed 23 Apr. 2019].

(d) About.att.com. (2019). AT&T, Sprint, T-Mobile and Verizon unveil next-generation mobile authentication platform details. [online] Available at: https://about.att.com/story/att_sprint_tmobile_and_verizon_unveil_next_generation_mobile_authentication_platform_details.html [Accessed 23 Apr. 2019].