BioSpectrum the business of Bio & Health Sciences

Time to embrace identity-based authentication for cybersecurity

19 September 2021 | Views | By Hemen Vimadalal, Founder and CEO, 1Kosmos, US

The healthcare and pharma sector can bring identity into the security infrastructure by eliminating passwords and instead opting for identity-based authentication

This year, we have seen numerous hospital systems under pressure while taking care of COVID-19 patients and facing ransomware attacks. Although hospital systems have faced ransomware attacks for years, this was the first time that these attacks were proven to cause patient harm. According to a study by the United States' Cybersecurity and Infrastructure Security Agency, patient health suffered more in hospitals that were facing a cyberattack than in hospitals that were not.

This is because hospitals that were already facing the stressor of COVID-19 did not have the capacity to fight a ransomware attack. We saw the detrimental impact the COVID-19 and ransomware attack combination had on patient health at many hospital systems including the University of Vermont Health Network. When their computer systems were hit by a ransomware attack in October 2020, they were unable to access health records electronically for a month. This delayed critical medical services like chemotherapy and cancer screenings.

How can these ransomware attacks be prevented? Organisations combat these attacks in a variety of ways from email security training, to prevent phishing, to adding Multi-Factor Authentication (MFA), but this has side effects. Users trained to spot phishing emails tend to report higher numbers of false positives to an already busy help desk. MFA adds friction. Neither solution is foolproof and nor do they solve the fundamental problem of knowing who is actually logged in behind the credentials.

Replacing passwords with biometrics gets another step closer, but again, unless the biometrics are tied to identity the fundamental user identity problem remains. Identity-based authentication solves this, but how then do we bring properly proofed identity into the security infrastructure?

This needs to be done in a way that doesn't compromise privacy and is user friendly. The healthcare and pharma sector can bring identity into their security infrastructure by eliminating passwords and instead opting for identity-based authentication. What does this look like in practice?

To identify ourselves in person, we use a credential, like a driver's license that is compared to our likeness. In the digital world, this type of identity verification happens during the friction-filled employee onboarding process. As many administrative functions have gone through digital transformation, employment eligibility verification is perhaps the poster child for inefficiency and waste because it's primarily manual, administration heavy and invested entirely on a one-time proof of identity.

By automating and modernising worker onboarding, we are able to create a reusable digital identity that can readily be used to authenticate workers at login. This has all the hallmarks of digital transformation, creating business efficiencies, speeding business process cycle time, reducing/eliminating costs, and preserving the investment in the form of a reusable identity. Perhaps most importantly, this allows us to improve security without compromising worker privacy. When a digital identity replaces login credentials like usernames and passwords, we call this next-generation multi-factor authentication.

This effectively protects organisations from breaches by preventing credential compromises. Also, implementing next-generation multi-factor authentication with biometrics moves your organisation towards a zero-trust environment. This means that identity is proven at every login. Creating a user-managed digital identity comes with numerous security benefits including the elimination of employee account takeover and reduced risk of personally identifiable information related data breaches. Additionally, replacing passwords with advanced biometric multi-factor authentication comes with operational benefits like improved user satisfaction. To truly eliminate the risk of ransomware, it's time to stop hoping for the best with password-based systems. Instead, decision-makers need to embrace identity-based authentication to strengthen their organizational security.

Hemen Vimadalal, Founder and CEO, 1Kosmos, US