1KOSMOS BlockID

Employee Onboarding: Eliminate Identity Compromises

Your organization conducting a security training, Then What?

Cybersecurity education needs to be on Human Resources' checklist during the onboarding process. But, at the end of the day, it's up to employees to put into practice what they've learned. When you know that 60 percent of employees in the U.S. reported sharing credentials with their colleagues, one may express doubts about the intrinsic pertinence of those security trainings [Source: Source: Verizon Data Breach Investigations Report, 2020]. Another staggering statistic adds to the credential sharing phenomenon: corporate insiders are responsible for 50 percent of data breaches. So, even though cybersecurity education is required, it's obviously not sufficient. When compiling a few cybersecurity curricula that US HR departments offer, one main topic stands out: adequate password management.

So, where does the problem lie exactly?

1 There Is No Such Thing as *Adequate Password Management*

There is a fact that anyone who's still leveraging passwords to access systems and applications, even as part of a 2FA or MFA solution, needs to integrate: 81% of data breaches are caused by poor password management [Source: Source: Verizon Data Breach Investigations Report, 2020]. Passwords can be forgotten, shared or stolen. A password is indeed the weakest link and yet the most important element of an authentication process in almost all Fortune 500 organizations today.

There are employees who have no problem remembering different usernames and passwords and will scrupulously follow what they've learned during their onboarding cybersecurity training. Unfortunately, the reality is that there are also those who give it three tries before they're locked out and start harassing the help desk. Finally, a few choose to rely on the good old post-it note they stick on their monitor, openly and publicly.

This ecosystem creates vulnerabilities, inefficiencies such as loss of productivity and increased costs. Did you know, for example, that replacing one password can cost up to $70? Yes, that's what it can cost in human capital and machine resources to handle one password reset request. But that's the best-case scenario, because a data breach can cost in the tens of millions of dollars.

1KOSMOS BlockID

Employee Onboarding: Eliminate Identity Compromises

2 The Only Solution: Go Passwordless, but That's Not Enough

Passwordless authentication solutions should leverage the user's smartphone as well as an advanced, unspoofable form of biometrics. In this situation, passwords are eliminated because the user uses something they have (their smartphone) and something they are (their biometrics).

What does unspoofable biometrics mean? Touch ID and Face ID are basic forms of biometrics that can be compromised or spoofed. An example of advanced, unspoofable biometrics is a liveness test. A liveness test requires users to capture a live video of themselves, during which they follow prompts (blinking of the eyes, smiling). If the liveness test doesn't match the liveness test the user initially performed during the enrollment process with the passwordless app, then the authentication fails.

The enrollment process is actually crucial to be able to verify the identity of the user indisputably. The enrollment of an employee must consist of triangulating a given claim (ID photo, address, last name, etc.) with a multitude of company or government-issued documents (driver's license, passport, etc.) as well as sources of truth (AAMVA, State Department, passport's issuing country, passport chip, credit cards, bank account, etc.), including the liveness test. By doing so, the passwordless solution can reach higher levels of identity and authentication assurance per the NIST 800-63-3 guidelines, or respectively IAL2 and AAL2.

3 What Does This Have to Do with Onboarding a New Employee?

The onboarding of a new employee includes key phases, from the verification of the new hire's identity for USCIS compliance purposes to the new employee's first login and corporate password reset, and during this journey there are eight opportunities of identity compromise. Two examples:

- A new hire must share government-issued documents as well as banking information with HR. In turn, Human Resources use the new employee's passport or a combination of his driver's license and his Social Security card to fill out the mandatory USCIS Form I-9 that verifies his employment eligibility in the United States. With the Covid-19 pandemic, it's likely the new employee is at home and consequently needs to scan and then email the documents or fax them directly. The consequence of this? His identity can be stolen as it travels unencrypted over the Internet.

Employee Onboarding: Eliminate Identity Compromises

- From the comfort of his home office, the new employee uses his username and complex password to access the company's systems and applications by connecting through his unsecure home wireless network, even though he was expressly told earlier to use his or her employer's VPN solution.

A mobile application that eradicates password authentication and onboards the employee by enrolling and verifying government documents in real-time eliminates the risk of identity compromises.

Conclusion

As an organization, you can choose to continue onboarding new personnel the same way and remain vulnerable to identity compromises throughout the entire process or become an agent of change and protect the integrity of your organization, its systems, and its workforce. The beauty about the latter is that with a solution like 1Kosmos, integration is completed in minutes, there is no software for you to install, and no technology for users to buy since they leverage their smartphones and simply need to download the BlockID app to get started.