princeton IDENTITY

SECURING DATA CENTERS WITH BIOMETRICS

PROBLEM

IN THE US, THERE WERE MORE DATA BREACHES IN THE FIRST NINE MONTHS OF 2023 THAN IN ALL OF 2021.[1]

While attacks are frequently launched from half a world away, others come from inside the physical facility where servers reside. Bad actors who gain physical access to a data center can tap into its computer networks even in a closed-loop environment.

In the US, there were more data breaches in the first nine months of 2023 than in all of 2021. While attacks are frequently launched from half a world away, others come from inside the physical facility where servers reside. Bad actors who gain physical access to a data center can tap into its computer networks even in a closed-loop environment.

Multi-factor authentication (MFA) has long been considered the best way to protect critical infrastructure, like data centers, from intruders. Recently, wily bad actors have found ways to circumvent traditional forms of MFA. Using phishing and social engineering, they lure unwitting credential-holders to accept false MFA verification requests, share information needed to redirect where SMS texts are sent, or answer personal knowledge questions. It happens at even the most sophisticated, tech-savvy workplaces. In August of 2022, a Cisco employee accepted a fake FMA request, allowing attackers into the company's critical internal systems.[2]

Companies need an infallible form of MFA to protect their data centers. Biometrics offers a promising solution.

SOLUTION

Biometric identity technology can be integrated within physical and logical security applications, creating a virtually impenetrable obstacle for imposters. Biometrics replace knowledge-based identifiers with physiological ones, like fingerprints, vein patterns, or facial geometry. Some biometrics are more precise and secure than others. For example, the patterns within the iris are so unique to each individual that a

[1] https://www.idtheftcenter.org/publications
[2] https://www.datacenterknowledge.com/security/cyberattacks-are-bypassing-multi-factor-authentication

false match occurs less frequently than once in one million. Furthermore, bad actors cannot reverse engineer an "iris" to match that of an enrolled user. When combined with other forms of authentication – a secondary biometric modality, a physical card or fob, a mobile credential, or a password, no more secure identity management solution exists.

An enrollee's biometric data may be stored on a 13.56 MHz access control SmartCard or a smartphone, eliminating the need for centralized storage of biometric data. To enter a secure area, a person must present a credential and match the biometrics stored on their card or phone.

Once inside a data center, biometrics can offer a convenient method to enforce zero-trust protocols. The "never trust, always verify" principle is burdensome for workers when they must manually and repeatedly enter passcodes. Biometric sensors attached to computer workstations or laptops can quickly verify a user's identity each time they interact with the network, streamlining logical access verification and authentication. They can also be deployed when remote access to data center servers is necessary.

Readily available APIs allow many biometric identity technologies to integrate seamlessly with today's electronic access control platforms, allowing for customized MFA solutions. Furthermore, some biometric identity system manufacturers now offer turnkey systems incorporating biometrics, card readers, and pin codes within a single reader device.

WHEN COMBINED WITH OTHER FORMS OF AUTHENTICATION – A SECONDARY BIOMETRIC MODALITY, A PHYSICAL CARD OR FOB, A MOBILE CREDENTIAL, OR A PASSWORD, NO MORE SECURE IDENTITY MANAGEMENT SOLUTION EXISTS.

security, convenience, and efficiency to tomorrow's commercial office space. Knowledgeable security integrators have the power to accelerate an adoption that will surely benefit a large segment of society.