How does IDEE prevent insider threats

IDEE GMBH

Table of contents

0 Glossary

- **Absolute Zero Trust (AID):** Supercharge Zero Trust Architecture by removing need to trust IDEE as the IDP and independently verify a user.
- **Mandatory device lock:** In order to use the authenticator app to login to a service the user is forced to have an active device lock on his phone.
- **MPA:** Protect modification of your most critical assets by requiring modifications to be approved by more than one person (digital 4-eye principle).
- **No manual data entry:** With IDEE's solutions there is no manual data entry for the user. The keys are managed in the secure storage of the app.
- **PKI:** Ensure users' authenticity by relying on a key-based infrastructure.
- **QR-Code:** Be on top of the user experience curve by making authentication as simple as scanning a QR code with the user's smartphone.
- **Remote logout:** Allow users to end a session remotely directly from their smartphone e.g., if they forgot to log out.
- **Self-service portal:** IDEE's Self-Service Portal is a default component that allows users to manage their accounts and devices themselves e.g., in case of a lost or stolen device. Users can easily delete devices, end sessions or delete their account when necessary from within an easy-to-use interface, accessible through a web browser.
- **Session identifier:** In order to detect and abort illegitimate requests unique random characters (word) help users to identify PUSH login request initiated by them.
- **Strong identity proofing:** Eliminate even the slightest chance of an administrator to intercept, fake or impersonate a user authentication request by directly tying user registration to the independent user verification of EZT
- **Truly passwordless:** Fully eliminate all password-related risks from your list of potential threats, as with AuthN™ there are simply no passwords.
- **Trusted device:** Ensure that individual authenticator devices can be trusted

1 Statistic

Usually network, and infrastructure attacks could be mitigated by using protections such as firewalls, anti-virus, patching, vulnerability management systems, and other proven approaches addressing existing vulnerabilities. However, credential-based attacks are the most prevalent threats for any organisation's security because credentials are used by people and humans fail, often. In fact, credentials were the object of more than 80% of cyber attacks reported in the Verizon 2020 DBIR.

2 Definition of Insider Threats (modified definition of NIST)

The threat that an insider (somebody within the organization, such as an employee, former employee, contractor or business associate) will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the company. This threat can include damage to the company through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

3 Insider Groups

Insider threats arise from two different groups of insiders:

Malicious insiders: people who wittingly take advantage of their access to inflict harm on an organization.

Negligent insiders: people who unwittingly make errors and disregard policies, which place their organizations at risk.

4 Marketing statements

IDEE **eliminates malicious insider threats** as a result of account compromise, ATO, unauthorized access through abuse of privileges, or authentication bypass . IDEE’s AuthN makes it impossible for the admin to manipulate or alter user credentials or to unilaterally make sensitive changes.

IDEE's AuthN **prevents unauthorized access due to employee's negligence** such as credential sharing, credential reuse, weak credentials, phishing and other credential related attacks.

5 Detailed explanation on malicious insider threats

IDEE eliminates malicious insider threats caused by…	**Feature or solution that eliminates the threat**
Account compromise	PKI, trusted device
ATO	Strong identity proofing
Bypassing by the IDP	Extended zero trust (AID)
Malware used to harvest credentials (e.g. keylogging and screen capturing malware)	PKI, truly passwordless, no manual data entry
Unauthorized access through abuse of privileged access	MPA

6 Detailed explanation on insider threats due to negligence

IDEE eliminates malicious insider threats caused by…	**Feature or solution that eliminates the threat**
Weak credentials (passwords)	PKI, truly passwordless
Password reuse (credential stuffing as a result)	PKI, truly passwordless
Credential sharing (two employees share the same password)	PKI, truly passwordless
Memorable credentials (passwords)	PKI, truly passwordless
Social engineering attacks geared towards obtaining credentials (phishing, spear phishing, ...)	no manual data entry, QR-Code, remote logout, session identifier
giving access to unattended devices	Remote logout

stolen/lost authenticator device	Mandatory device lock, self-service portal