Das Schlüssel-Element Ihrer Cyber-Security.

SIE WOLLEN IHR UNTERNEHMEN VOR CYBER-ANGRIFFEN SCHÜTZEN? ABWEHR VON UNAUTORISIERTEN ZUGRIFFEN MITTELS GESTOHLENER BENUTZERDATEN IST FÜR SIE WICHTIG? SIE WOLLEN SCHWERWIEGENDE RECHTLICHE UND FINANZIELLE FOLGEN VERMEIDEN?

Ob gestohlene Firmen- oder Kundendaten – Cyber-Kriminalität hat sich zu einem lukrativen Geschäft entwickelt. Oftmals gelangen diese Cyber-Kriminellen über die eigenen Mitarbeiter unbewusst in das Unternehmenssystem: Denn rund 76 %* aller unbefugten Netzwerkzugriffe erfolgen über schwache oder gestohlene Benutzerdaten.

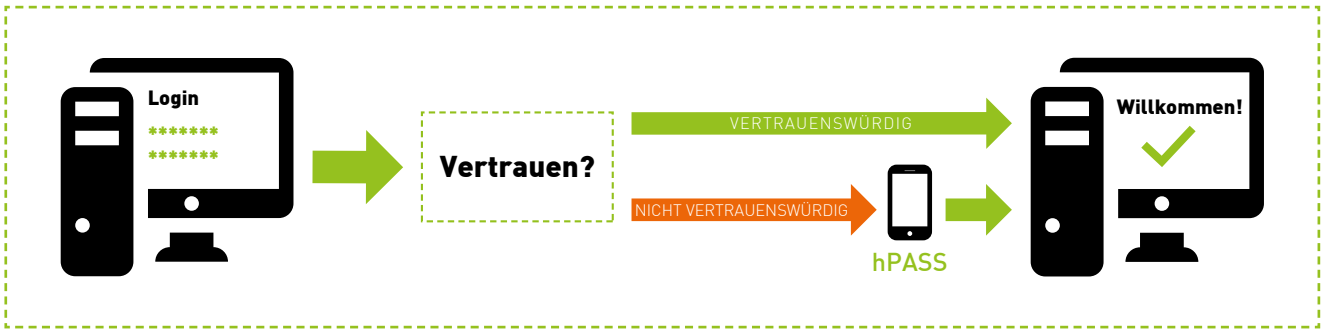
Angesichts dieser Bedrohung und der ständigen Verfügbarkeit und Zugriffsmöglichkeit Ihrer IT-Infrastruktur, wird der Bedarf an sicheren und wirkungsvollen Authentifizierungsmethoden immer größer. Bislang verwendete Hardwaretoken oder einfache mobilfunkbasierte Lösungen tun sich schwer, moderne Cyber-Gefahren abzuwehren und gleichzeitig den Anforderungen an eine hohe Benutzerfreundlichkeit zu genügen.

hPASS – BENUTZERFREUNDLICHE MULTI-FAKTOR-AUTHENTIFIZIERUNG

WEGBEREITER EINER NEUEN GENERATION DER BENUTZERAUTHENTIFIZIERUNG

hPASS, das Managed Service von Huemer Data Center, sperrt Hacker erfolgreich durch adaptive Multi-Faktor-Authentifizierung aus – selbst dann, wenn diese Ihr Passwort bereits geknackt haben. Starke Sicherheit für Ihr Unternehmen mit höchstem Benutzerkomfort: hPASS nutzt den einen Gegenstand, den Anwender stets bei sich tragen – das Mobiltelefon.

Per sicherer Flash-SMS erhalten Benutzer stets ein echtzeit-generiertes Einmalpasswort zur unkomplizierten und einfachen Authentifizierung. Somit gewährleistet hPASS hohen Schutz und ist dabei so intuitiv und bequem zu bedienen, dass das Einhalten von Sicherheitsanforderungen zum Kinderspiel wird.



*Quelle: 2013 Data Breach Investigations Report von Verizon

Huemer Data Center Ges.m.b.H. | Leonard-Bernstein-Str. 10, 1220 Wien | T +43 1 26 33 770 - 0 | E sales@huemer-dc.com

Das Schlüssel-Element Ihrer Cyber-Security.

hPASS – BENUTZERFREUNDLICHE MULTI-FAKTOR-AUTHENTIFIZIERUNG

NAHTLOSE INTEGRATION

hPASS lässt sich nahtlos in Ihr Anmeldesystem integrieren und bietet damit eine intuitive und anwenderfreundliche Lösung für die Remote- oder Cloud-Anmeldung.

ADAPTIVE AUTHENTIFIZIERUNG

hPASS verbindet auf optimale Weise höchste Sicherheit und Benutzerakzeptanz. Die erforderliche Authentifizierungsebene wird auf Basis der Bedrohungsstufe automatisch angepasst – je nachdem von wo, wann oder über welches Netzwerk die Anmeldung erfolgt.

FLASH-SMS

hPASS versendet Passwörter standardmäßig als Flash-SMS. Diese werden automatisch direkt auf dem Mobiltelefon des Benutzers angezeigt, dort jedoch nicht gespeichert. Der Versand einer gewöhnlichen SMS kann optional gewählt werden.

STANDORT- UND VERHALTENS-ABHÄNGIGE SICHERHEIT

hPASS nutzt Kontextdaten wie Anmeldeverhalten und Standort-Informationen des Benutzers vollständig, um auf diese Weise effektiv Zugriff zu gewähren oder zu verweigern.

LEICHT LESBARE EINMAL-PASSWÖRTER

hPASS stellt durch die innovative Nutzung von Buchstabenkombinationen den Benutzern leicht lesbare Einmalpasswörter bereit, die den intuitiven Anmeldeprozess unterstützen. Die Einmalpasswörter werden von geprüften Crypto-Modulen erzeugt.

IHRE VORTEILE IM ÜBERBLICK

Schnell
- Innerhalb weniger Minuten einsatzbereit
- Nahtlose Integration für Remote- oder Cloud-Zugriff
- Geringer Aufwand auf Kundenseite

Einfach
- Installieren, integrieren, verwalten, skalieren, verwenden
- Integration in das Active Directory (ohne Schema-Änderungen oder Schema-Erweiterungen)
- Einfaches Anlegen neuer Benutzer
- Keine Bereitstellung neuer Software erforderlich
- Keine Mitarbeiter-Schulungen notwendig
- Auf allen Gerätetypen anwendbar

Günstig
- Kostengünstige Multi-Faktor-Authentifizierung
- Geringer Aufwand für Installation und Administration durch Managed Service
- Keine Investitionskosten
- Niedrige Gesamtbetriebskosten
- Kosten durch All-Inclusive-Modell genau planbar

Sicher
- Hosting in zertifizierten österreichischen Rechenzentren von Huemer Data Center
- Lösung arbeitet in Echtzeit
- Keine vorgefertigten Passwörter oder Seed-Dateien
- Zufällig generierte Einmalpasswörter
- Echtzeit-Benachrichtigung bei Phishing oder Man-in-the-Middle Angriffen
- Schutz vor Brute-Force- und Denial-Of-Service Angriffen
- Verschlüsselung jeglicher Kommunikation
- Versendung der Passwörter via Flash-SMS
- Individuelle Konfiguration (Authentifizierungsebene)

Huemer Data Center Ges.m.b.H. | Leonard-Bernstein-Str. 10, 1220 Wien | T +43 1 26 33 770 - 0 | E sales@huemer-dc.com