DIGITAL AGENTUR BERLIN

DAB Cyberwerkstatt

Wiederbenutzt wird ausgenutzt! Prävention durch Passwort- & Accountsicherheit

Die Veranstaltungsreihe „DAB Cyberwerkstatt“ vermittelt auf praktische Weise Basiswissen zum Schutz der IT-Infrastruktur Ihres Unternehmens. In dieser Ausgabe geht es um die Themen Passwort- und Accountsicherheit und was Sie in Ihrem Unternehmen tun können, damit die Bedienerfreundlichkeit nicht unter der Sicherheit leidet oder umgekehrt.

Agenda

1.	**Begrüßung & Vorstellungsrunde**	**20 Min**
2.	**Impulsvortrag Accountsicherheit**	**25 Min**
–	**Warum Accountsicherheit?**	
–	**Wie werden Konten gehackt?**	
–	**Was macht ein sicheres Paswort aus?**	
3.	**„MFA“ – eine spielbasierte Lerneinheit**	**25 Min**
	Pause	**15 Min**
4.	**MFA und weitere Sicherheitsmethoden**	**30 Min**
5.	**Ihre nächsten Schritte: DAB Checkliste**	**5-10 Min**
6.	**Zeit für Fragen**	**10 Min**
	Checkout ...anschließend Zeit zum Austausch	

Glossar

Account / User-Account	Nutzerkonto; Zugangsberechtigung zu einem IT-System
Biometrie	Altgriech. von „Leben“ und „Maßstab“; in diesem Zusammenhang Wiedererkennung anhand einzigartiger körperlicher Merkmale, wie Fingerabdruck, Gesicht oder Iris im Auge
Brute Force	(engl. „rohe Gewalt“); ausprobieren aller denkbaren Möglichkeiten
Credential Stuffing	Cyberangriff unter Verwendung im Vorfeld erbeuter Zugangsdaten
Hardware-Key	auch Dongle, Hardlock oder Kopierschutzstecker; ist ein Datenträger, auf welchem Anmeldeinformationen gespeichert sind, die ähnlich wie Schlüssel und Schloss verwendet werden
Hash-Wert	(von engl. (to) hash = zerhacken); Algorithmus zur Verschlüsselung; Schriftzeichen werden einem Wert zugeordnet und zusammengerechnet (Vgl. Quersumme)
Login	(von engl.: (to) log in = einloggen, anmelden); Benutzer-Anmeldung, auch: Sign-in/Sign-on, Log-on
Keylogger (engl. „Tasten-Rekorder“)	ist eine Software oder Hardware, die Tastatureingaben protokolliert, wie z.B. Nutzernamen und Passwort.
Multi-Faktor-Authentifizierung (MFA)	auch -Authentisierung, oder auch 2-Faktor-A. (2FA) sind mehrstufige Anmeldeverfahren, bei denen zur Sicherheit mindestens ein zweiter Faktor benötigt wird
Passwort	oder Kennwort, Codewort, Schlüsselwort; Schutzmaßnahme zur Authentifizierung berechtigter Benutzer, „ein gemeinsam bekanntes Geheimnis“
Passwort-Manager	auch Passwortsafe/ -tresor; eine Software in der verschiedene Passwörter sicher verwaltet werden können
Passwort-/ Account-Sicherheits-Richtlinie	oder -Policy sind verbindliche Vorgaben, wie Passwörter beschaffen sein müssen und was im Umgang damit zu beachten ist; eine PW-Policy kann auch systemisch eingestellt werden
PIN	Persönliche Identifikationsnummer, ein Passwort das in der Regel nur aus Ziffern besteht
Secure-Shell (SSH)	kryptographisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten
Sicherheitsfragen	Authentifizierungsmethode, die z.B. bei Passwort-Rücksetzungen verwendet werden und darauf basieren, dass nur berechtigte Nutzer die korrekte Anwort kennen, Bsp. „Wie lautet der Mädchenname Ihrer Mutter?“
Single-Sign-on (SSO)	Zentraler Anmeldedienst für mehrere Anwendungen
TAN	Transaktionsnummer; ein Einmal-Kennwort, vorwiegend aus dem Online-Banking bekannt
Token	auch Security- oder Software-Token; weitere Form der MFA bei der dem berechtigten Nutzer ein zeitlich befristetes Einmalkennwort zur Authentifizierung übertragen wird

1. Welche Punkte sind im Rahmen einer Bestandsaufname zur Accountsicherheit im eigenen Unternehmen relevant?

Gibt es eine Übersicht, welche Anwendungen User-Accounts (Nutzerkonten) verwenden?

- Haben Nutzer individuelle Anmeldungen oder nutzen alle dieselbe?
- Enthält die Anwendung sensible Informationen, wie Bankdaten?
- Unterstützt die Anwendung sichere Passwörter?
- Gibt es Möglichkeiten für MFA?

Gibt es ein Rechte- und Rollenkonzept?

- Ist definiert, wer welche Berechtigungen haben muss?
- „Minimalprinzip“ oder „Need-to-know“/ „Need to use“

Werden Berechtigungen von Accounts regelmäßig kontrolliert?

- regelm. Aktualisierung bei Positionswechsel und besonders bei Austritten?
- Werden Konten bei längerer Inaktivität automat. oder manuell gesperrt?

Verfügt Ihr Unternehmen über eine Passwort-/ Account-Sicherheits-Richtlinie?

- Ist festgelegt und dokumentiert, wie Passwörter beschaffen sein müssen?
- Ist definiert, was grundsätzlich bei Anmeldungen zu beachten ist?
- Sind alle Nutzer dazu belehrt, bei Anstellung und danach regelmäßig?

Besteht ein Sicherheitsbewusstsein gegenüber Phishing?

- Wissen Mitarbeitende, wie sie sich verhalten?
- Ist die Systemlandschaft darauf ausgelegt, Phishing auszusperren?
- E-Mail-Sicherheit unterstützt Accountsicherheit

IT-Notfallplan für alle IT-Sicherheitsvorfälle

Regelemäßige Überprüfung/ Schulungen der Mitarbeitenden

Denken Sie daran: *Ihre „Sicherheitskette“ ist nur so stark wie ihr schwächstes Glied*

Platz für Ihre Notizen:

2. Wie werden Passwörter am häufigsten geknackt?

1. Brute-Force-Angriffe: Alle möglichen Kombinationen von Zeichen werden probiert, bis zum richtigen Ergebnis.
2. Wörterbuch-Angriffe: Durchprobieren von Listen mit häufig verwendeten Passwörtern, Phrasen oder Kombinationen
3. Gestohlene Passwort-Hashes: Wenn Passwort-Hashes gestohlen werden, können sie entschlüsselt werden, um das Passwort zu erhalten.
4. Keylogger: Schadsoftware zeichnet Tastatureingaben auf, um das Passwort zu stehlen.
5. Social Engineering: Gezielte Täuschung um das Passwort von Nutzern zu erhalten.
6. Credential Stuffing: ……

   …….

3. Wie sehen sicherere Passwörter aus?

Die Szenarien 1 – 3 können durch die Verwendung möglichst langer, komplexer Passwörter verhindert werden. Das heißt:

- Mindestens 12 Zeichen, bei sensiblen Inhalten mindestens 16
- Groß- und Kleinbuchstaben, Sonderzeichen, Zahlen
- Keine einzelnen Wörter aus dem Wörterbuch
- Für jeden Account individuelles Passwort & Benutzername
- Bei Zahlungsdaten & sensiblen Informationen reichen Nutzername + PW nicht aus
- Logins nicht aufschreiben oder weitergeben

Gegen die Szenarien 4 und 5 helfen Sicherheitssoftware und Schulungen der Mitarbeitenden.

Platz für Ihre Notizen:

4. ALARM Serious Game: „Multi-Faktor-Authentifizierung“

Hat Ihnen das Spiel gefallen? Auf der Projektseite der Technischen Hochschule Wildau können Sie dieses und weitere analoge oder digitale Awareness Games nutzen oder herunterladen, um sie z.B. als Schulungsmethode in Ihrem Unternehmen zu verwenden.

Platz für Ihre Notizen:

5. MFA und weitere sichere Anmeldemethoden

z.B. Fingerabdruck oder Gesichtserkennung

Zugesendet per SMS oder E-Mail

mit einem Smartphone z.B.

TOTP: time-based one-time password z.B. über eine Authenticator-App

Anmeldedaten sind auf Datenträger gespeichert, der zum Entsperren an-

gesteckt wird

z.B. auf ein Smartphone

wird für passwortlose Anmeldung mittels PassKey verwendet oder bei SSH (Secure Shell) mit keygen

Platz für Ihre Notizen:

6. Wie funktionieren Passwortmanager oder Hardware-Key?

Um verschiedene, möglichst lange, komplexe Passwörter für alle Anwendungen nutzen zu können, ist ein Passwortmanager zu empfehlen. Mit einem Master-Passwort werden alle weiteren Einträge in der Passwortdatenbank verschlüsselt. Damit muss man sich nur noch das eine Masterpasswort einprägen.

Eine weitere Methode, die man in Kombination mit dem Passwortmanager oder mit anderen Anmeldemethoden benutzen kann, sind Hardware-Keys. Die Logindaten sind dabei fest auf einem Datenträger (z.B. USB-Stick) gespeichert und werden zur Entsperrung angesteckt. Die Sicherheit basiert auf dem physischen Besitz, der für Cyberkriminelle aus der Ferne nicht erreichbar ist.

7. Ihre nächsten Schritte: DAB Checkliste

Mithilfe unserer Checkliste, die Sie im Nachgang erhalten können Sie in Ihrem Unternehmen prüfen, ob in der genutzten Software sicherer Nutzerkonten bestehen, wie wir am Beispiel erläutern.

Wie sicher sind Anwendungen mit Nutzerkonten?

Rechnen Sie die Punkte zusammen, wenn das Kriterium zutrifft:

Software/ Online - Anwendung	Personal-Tool	Website						Punkte
Sensibler Inhalt[1]	-5							-5
Personalisierte Logins[2]	+1							+1
Gruppen-Logins[3]		-3						-3
Rollen-Rechte-Konzept[4]	+1	+1						+1
Passwort-Policy[5]	+1							+1
Regelm. PW-Änderung[6]								0
Single-Sign-On (SSO)[7]								+1
Multi-Faktor-Authent.[8]	+2							+2
User deaktivieren[9]								+1
Löschen/ rezertifizieren[10]	+1							+1
	= 1	= -2						

Ergebnis: größer als 0: sehr gut | gleich 0: okay | kleiner 0: Zeit zu handeln

Platz für Ihre Notizen:

Vielen Dank für Ihre Teilnahme!

In Kürze erhalten Sie von uns alle Unterlagen aus der heutigen DAB Cyberwerkstatt per E-Mail zugeschickt.

Wenn Sie im Nachhinein noch Fragen haben sollten, kommen Sie jederzeit gerne auf uns zu und vereinbaren Sie ein kostenfreies DAB Orientierungsgespräch oder besuchen Sie unsere Veranstaltungen, online oder vor Ort.

Die Digitalagentur Berlin in Sozialen Medien:

LinkedIn:
@DAB Digitalagentur Berlin

Instagram:
@digitalagentur.berlin

YouTube:
@Digitalagentur Berlin