Kennwort-Sicherheit

Aktuelle Analyse, Patrick Bärenfänger, V1.31, September 2021

PBCS

Patrick Bärenfänger

Lebenslauf

- 1969 geboren, Ausbildung DV-Kaufmann, Studium Elektrotechnik/Informatik
- Seit 1990 in der EDV-Branche als PBCS
- Von 1995-2001 GAO Münster (Ratiodata IT-Lösungen und Services GmbH)
- 2001 in Projekten für Microsoft, AXA-Colonia, Döres AG, und GAD eG
- Seit Januar 2002 bei der GWS in Münster

- Schwerpunkt Informationssicherheit und IT-Ausbildung
  - IT-Security Manager und Auditor (TÜV zertifiziert)
    - Datensicherheit (Symantec und Veritas SSE+ zertifiziert)
    - Infrastruktur-Bewertung (Citrix CCSP und Microsoft zertifiziert)
  - Systemkoordinatoren-Schulung und Zertifizierung
  - Softwarepaketierung, Lizenzierung
  - Test und Einführung neuer Produkte

Rund 30 Jahre IT-Erfahrung

Kennwort-Sicherheit

Ausgangslage

- Das Bundesamt für Sicherheit in der Informationstechnik gibt in den Grundschutz-Katalogen (speziell: 200.1) Anweisungen, wie Unternehmen ein Mindestmaß an Sicherheit erreichen können.
- Im Prüfungsstandard 330 vom Institut der Wirtschaftsprüfer sind ähnliche Empfehlungen zu finden

- Viele Hersteller und Lieferanten verwenden „Werks-Kennwörter" für Ihre Geräte und Software
  - WLAN-Router von AVM und der Telekom haben einen unsicheren Werks-Schlüssel auf dem Gerät aufgedruckt

- Viele Kunden verwenden Werkskennwörter weiter oder erlauben den Mitarbeitern, unsichere Kennwörter zu verwenden

- Organisatorische Maßnahmen (z. B. bei Austritt eines Mitarbeiters) sind nicht dokumentiert und/oder werden nicht umgesetzt

- Die operative Verantwortung, Umsetzung und Einhaltung der Kennwortrichtlinien liegt beim Systemkoordinator, gesamtverantwortlich ist die Geschäftsleitung.

Kennwort-Klassen

Wir unterscheiden zwischen verschiedene Klassen von Kennwörtern (die Zahl in Klammern misst das Risiko durch Missbrauch):

- Benutzer-Kennwörter, die nur hausintern funktionieren (1)
- Benutzer-Kennwörter, die auch über das Internet eingegeben werden können (Exchange Web App, Push-E-Mail auf Smartphones, VPN-Zugang (3)
- Benutzer-Kennwörter mit Zugriff auf Lohn und Personaldaten (6)
- Geräte-Kennwörter mit Zugriff nur über das lokale Netzwerk (Switches, Kameras, Wartungsklappen der Server IRMC) (2)
- Administrative Kennwörter (Lokaler Server oder Domänenweit) (5)
- Dienste Kennwörter und Kennwörter in Softwareprodukten (Datensicherung, Warenwirtschaft, Archiv, Banking, Fahrerkarten, Zeiterfassung und viele mehr) (4)
- WLAN-Passphrases (7) – Hackmöglichkeit in Sende-Reichweite des Access-Points

Kennwort-Sicherheit

Risiken (Fallbeispiele)

- Administrator verlässt das Unternehmen
  - Ist das Admin-Kennwort Werkspasswort → hohes Risiko
  - entspricht das Admin-Kennwort den BSI Sicherheits-Anforderungen → mittelschweres Risiko

- Mitarbeiter ohne Sonderrechte verlässt das Unternehmen
  - Mitarbeiter-Konten werden nicht deaktiviert → hohes Risiko wenn Geldverkehr möglich (Kassenlade), hohes Risiko für Datendiebstahlt
  - Mitarbeiter Kennwörter werden nicht zurückgesetzt

- Mitarbeiter haben unsichere Kennwörter
  - Beliebte Kennwörter lauf Analyse: 1234 xxxx 123456 gevis <Name des Hundes> <Name des Kindes> <Automarke> → Risiko des Datendiebstahls und Missbrauchs durch andere nicht berechtigte Mitarbeiter

- Mitarbeiter haben unsichere Kennwörter und Pushmail/ Exchange Zugriff über das Internet
  - → Datendiebstahl, Identitätsdiebstahl

Generell: Gesetzesverstöße bis ins Strafrecht, Verstöße gegen Datenschutzvorschriften (BDSG und DS-GVO)

Kennwort-Sicherheit

Sichere Kennwörter?

Je nach Risikoklasse (1-7) müssen Mindest-Anforderungen für Sicherheit sorgen. BSI-Grundschutz-Empfehlungen (M 2.11) gelten als Maß der Dinge:

- Administrative Kennwörter:
  - Mindestens 8 Zeichen
  - 2 von 3 aus (Sonderzeichen, Groß/Kleinschreibung, Zahl)
  - Änderungspflicht unmittelbar nach Austritt Administrator oder wenn Kennwort „verbrannt“ ist
  - Regelmäßige Änderung nicht möglich, wenn Windows-Dienste administrative Konten verwenden
  - → Separate Named User Adminkonten für die Administratoren erzeugen, dann ist eine regelmäßige Änderung möglich

- Benutzer-Kennwörter:
  - Mindestens 6 Zeichen
  - 2 von 3 aus (Sonderzeichen, Groß/Kleinschreibung, Zahl)
  - Kennwort-Historie: 20 Kennwörter
  - Empfehlung des BSI, Kennwörter alle 90 Tage zu ändern (alte Empfehlung, führt zu unsicheren Kennwörtern als ohne Änderungszwang)

- WLAN-Kennwörter (betrifft alle Geräte, die Kennwort-Brute Force ermöglichen)
  - Mindestens 26 Zeichen
  - 3 aus 3 (Sonderzeichen, Groß/Kleinschreibung, Zahl)

Kennwort-Sicherheit

Warum sind Kennwörter, die regelmäßig geändert werden müssen, unsicherer?

- Studien von mehreren Universitäten und eine wissenschaftliche Ausarbeitung vom National Institute for Standards (US-Standard-Behörde) von 2017 belegen:

- **Von regelmäßiger Kennwort-Änderung wird ausdrücklich abgeraten**
  - Es gibt keine technische Richtlinie, die den Benutzer zwingt, völlig unterschiedliche Kennwörter zu verwenden
  - Wenn Mitarbeiter Kennwörter regelmäßig ändern, verwenden sie verwandte Kennwörter zum Ursprungskennwort
  - Es werden Kennwörter aus Wörterbüchern gebildet
  - Beispiele: Biber11$, dann Biber12$ usw.

- Kennwörter aus mehreren unsinnigen Wörtern sind sicherer als ein kurzes komplexes Kennwort:
  - dehR Bferd frizt 95 saK hafeR ← sicherer als (aber unkomfortabler)
  - &GeB2hT1

Kennwort-Sicherheit

Maßnahmen und Empfehlungen

- Bestandsaufnahme im eigenen Unternehmen durchführen oder beauftragen
  - Beim IT-Sicherheits-Check und bei IT-Systemprüfungen werden Fehler oft bemängelt, es wird aber auch dann nicht gehandelt)

- Administrative Konten anlegen, die der natürlichen Person „Systemkoordinator" zugeordnet sind (Regelmäßige Änderung dann möglich, wenn gewünscht)
- Dienste-Konten mit sicheren Kennwörtern ausstatten, die nur bei Notwendigkeit geändert werden
- Richtlinie für Benutzer-Kennwörter gemäß BSI-Grundschutz implementieren
- Organisatorisch: Mitarbeiter sensibilisieren, sichere, geheime Kennwörter zu verwenden
- Wenn gewünscht, Windows-Kennwörter alle 90 Tage zu ändern erzwingen
- Exchange: Nur Mitarbeiter für OWA und Push-Email zulassen, die diesen Zugang nutzen müssen/dürfen
- WLAN: Passphrases auf mindestens 26 Zeichen und komplex generieren, wenn möglich mit Client Zertifikaten arbeiten (AD-Zert). Zum WPA2-Protokoll gibt es noch keine sicherere Alternative!
- Internet-Zugänge: Wenn möglich und vom Anbieter unterstützt: 2-Faktor-Authenfizierung verwenden, ansonsten dort nur sichere und eindeutige Kennwörter verwenden
- Web-Kennwörter im Keepass-Passwort-Safe speichern und diesen mit 2-Faktor absichern (Schlüssel und Master-Kennwort)

Kennwort-Sicherheit

Werkzeuge

- Kennwort-Generator (überträgt keine Daten über das Internet, da er als JSCRIPT auf dem lokalen Rechner in der Browser-Sandbox läuft). Kennworte erzeugen lassen oder eingeben und bewerten lassen:
  - Auf pbcs.de

- Keepass Passwortsafe (speichert Kennwörter hochverschlüsselt in einer lokalen Datei und **nicht** im Internet oder der Cloud). Auch die Android App verwendet diese lokale Datei auf der Speicherkarte des Smartphones)

- Sicherheitsmeldungen und Artikel im Heise Security Ticker verfolgen oder auf unserer Webseite im Blog: https://pbcs.de

Patrick Bärenfänger

Consulting & Solutions

Auf der Worth 4
59192 Bergkamen

Tel.: +49 (2307) 299 607
Mobil: +49 (171) 747 9294
Fax : +49 (2307) 299 765

E-Mail: patrick@pbcs.de

pbcs.de

Vielen Dank für Ihre Aufmerksamkeit
Zeit für Ihre Fragen