Forced Forcing©

Innovativster Schutz für alle Passwörter und wissensbasierte Authentifizierungen

Bulletin 2024

cyberbreeze

Zusammenfassung: *Forced Forcing©*

- **Passwortschutz** wird in den nächsten Jahren aufgrund zunehmender Remoteanwendungen und besseren technischen Angriffsmöglichkeiten massiv an Bedeutung gewinnen
- Mit ***Forced Forcing©*** haben wir eine einzigartige, patentierte Methodik, um die **Sicherheit in Potenz** zu steigern
- ***Forced Forcing©*** reduziert praktisch **alle Passwortrisiken** extrem sicher und kostengünstig
- Es ist enorm **schnell installiert** und braucht im Gegensatz zu vielen anderen Applikationen und Verfahren **keine Veränderungen** beim Nutzer und/oder dessen Kunden
- Wir werden ***Forced Forcing©*** daher in kurzer Zeit zum **globalen Standard** entwickeln

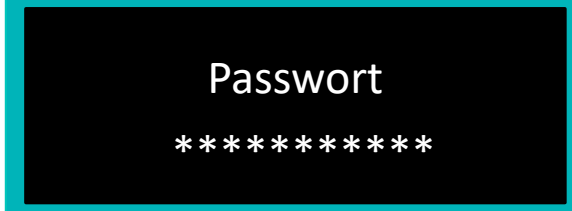
Durch COVID-19 explosionsartiges Wachstum von

- e-Commerce
- Online- und Mobile-Banking
- Homeoffice, Home-Schooling und Bildung
- Digitale Verwaltung und Behörden
- Videoservices und -konferenzen etc.

Neue Technologien und digitale Angebote u.a. bei(m)

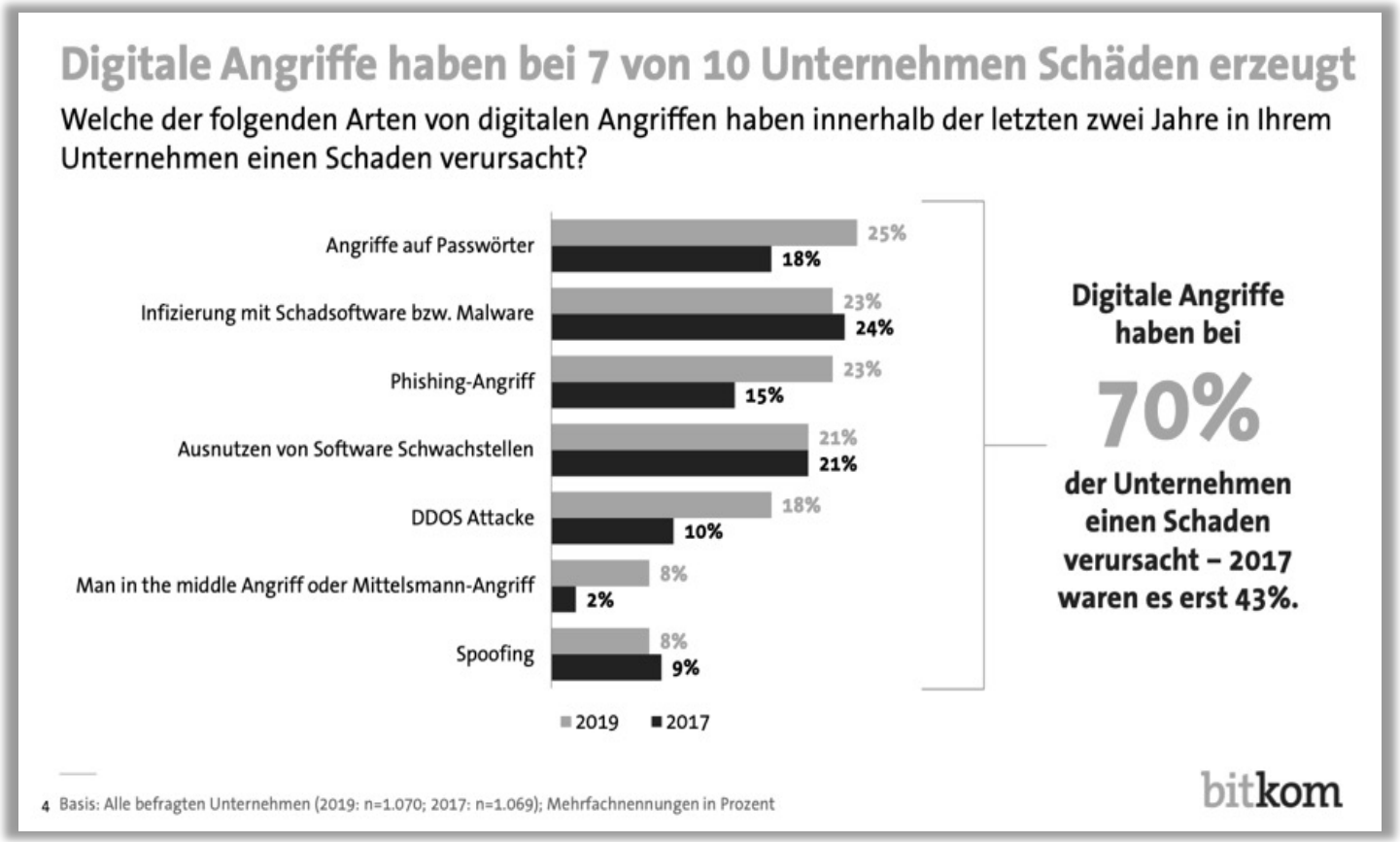
- Identitätsmanagement
- Digitalen Gesundheitswesen
- Blockchain, Krypto und Plattformökonomie
- IoT/5G
- Smarthome etc.

Achtung: Hochleistungsrechner, Quantencomputer und Botnetze ermöglichen Cyberattacken in einer neuen Dimension



Ca. 300 Mrd. Passwörter weltweit bedeutet die klare Nr. 1 bei der Authentifizierung – Tendenz steigend

Analysen zeigen: Die Gefahr wächst!



Schäden von ca. 230.000.000.000 EUR in Deutschland allein in 2021

cyberbreeze

Alle Authentifizierungsverfahren haben erhebliche Schwächen

Verfahren:	Bewertung:
Wissen („Knowledge“) Passwörter, PIN, grafischer Elemente oder Antwort auf eine Frage	**Unsicher**, da das menschliche Gehirn mit den zunehmenden Anforderungen an notwendiger Komplexität und Menge von Passwörtern überfordert ist
Besitz („Ownership“) Geräte, Smartcards, Token usw.	**Unsicher**, da Besitz entwendet, kopiert, oder gehackt werden kann
Inhärenz („Inherence“) Biometrische Merkmale	Bequem aber **unsicher**, da aufzeichenbar und mit Technologie zunehmend kopierbar

Risiken durch Hochleistungsrechner & Quantencomputer signifikant steigend.

Zunehmende Rechnerleistung macht Passwortschutz jetzt noch notwendiger

Brute Forcing: Durchprobieren von unzähligen nur noch schwer erfassbare Mengen von Passwörtern mit heutigen Hochgeschwindigkeitsrechnern oder Botnetzen

Dictionary Attacks: Durchprobieren von bis zu 100.000 gebräuchlichen Worten, Namen und Begriffen in Sekundenbruchteilen

Pattern/Combined Attacks: Suchen nach Mustern in Kombinationen von Buchstaben, Zahlen und Zeichen z. B. „H@nnover21“

Passwort Sprays/Database Attack: Automatisiertes Durchprobieren häufig genutzter Passwörter wie „Geheim123!“ bei allen Anwendern einer größeren Anwenderbasis

Interface Attacks/Offline Attacks: Zugriff auf den Hashwert von Passwörtern, so dass dieser offline bzw. mit erheblicher Rechnerleistung zum knacken des Passworts genutzt werden kann – bei passwortverschlüsselten Zip-Dateien ist dies schon systemisch möglich

Alternative Attack Vectors: Die Nutzung von Masterpassworten öffnet einem Angreifer einen neuen Angriffsvektor, nämlich den Angriff auf die Passwortverwaltung selbst:
Gelingt ihm dieser, hat er gleich alle Passwörter auf einmal kompromittiert

Die Lösung: *Forced Forcing©*

Forced Forcing© = Gedächtnisvermögen x Rechenleistung

Forced Forcing© = Gedächtnisvermögen x Rechenleistung

- Das **menschengemerkte Passwort** (bzw. die menschengemerkte Information im allgemeinen Fall) wird durch einen **zweiten, zufällig generierten Teil** quasi maschinell ergänzt
- Der Anwender muss sich diesen **zweiten Teil nicht merken**, kann ihn sogar völlig ignorieren und muss nicht einmal von seiner Existenz erfahren
- Stattdessen wird sein **eigenes Computersystem** bei jeder legitimen Authentifizierung gezwungen (*forced*), das eigene Passwort auf Basis des eingegeben, gemerkten Passwortteiles mittels **Brute Forcing** zu ermitteln
- Dabei wird die Länge sowie Komplexität des zusätzlichen zufälligen Teiles so gewählt, dass sie die **Rechenleistung des Anwendersystems** nur moderat belastet
- In der Praxis bedeutet das heute, dass ein gebräuchliches Mobiltelefon oder ein einfaches Notebook in **einer Sekunde einige Millionen Passwortmöglichkeiten** durchprobieren kann und muss
- Die Anwendererfahrung wird also **nicht** signifikant **beeinträchtigt**, die **Sicherheit** aber buchstäblich **exponentiell erhöht**

Einfache Passwortgenerierung und kombinierte Authentifizierung

1. **Passwortgenerierung:**
   - Der Nutzer generiert und merkt sich ein Passwort: **`sus@Nne42;`**
   - Das System des Nutzers generiert ein zusätzliches und völlig zufälliges Passwort z. B. aus sechs Zahlen. Dies bedeutet, dass das Nutzerpasswort in Kombination um den Faktor 1 Mio. sicherer wird: **`738482`**
   - Nach der Generierung des Passwort-Hash kann die zufällig generierte Passwortkomponente verworfen werden; eine etwaige Speicherung ist nicht erforderlich
2. **Legitimierung und Authentifizierung:**
   - Der Nutzer gibt wie gewohnt sein Passwort ein: **`sus@Nne42;`**
   - Mit Hilfe von Brute Forcing findet das System des Nutzers die zweite – also zufällig generierte und nicht gespeicherte Komponente des Passworts: `000000` … `999999` -> **`738482`**
   - Das System des Nutzers identifiziert sich im Zielsystem mit dem kombinierten Passwort: sus@Nne42;738482

Durch Kombination der zwei Passwortkomponenten steigt die Sicherheit exponentiell

Zeitdauer des Angriffs auf:	Zeit für Anwender	Zeit für Angreifer
Gutes Passwort (gängige Passwortregeln/best practices) ***(Gedächtnisvermögen)***	nicht erforderlich	**ca. 1 Stunde** **=> praktikabel machbar**
Forced-Forcing-Teil ***(Rechenleistung)***	**ca. 1 Sekunde** (erzwungen „forced“)	nicht möglich, da nicht separat angreifbar
Kombinierter Schutz ***(Gedächtnisvermögen x Rechenleistung)***	nicht erforderlich	**ca. 228 Jahre** **=> Angriff ist nicht realistisch durchführbar**

Ein Pentest im Auftrag einer internationalen Versicherungsgruppe bewies die Wirksamkeit von Forced Forcing ©. Ein unabhängiges wissenschaftliches Institut wird diese ebenfalls untersuchen und testieren.

Annahmen im Beispiel:

- *Offline-Angriff auf Hash ist möglich (=> hohe Angriffsgeschwindigkeit)*
- *Rechenleistung Angreifer 300 Mrd. hashes/sec (z.B. 5 Amazon p3.16x large instances)*
- *Rechenleistung Verteidiger 2 Mio. hashes/sec (z.B mid-range Smartphone)*
- *Gutes Passwort, entsprechend gängiger Passwort-Regeln (entspricht Resilienz von ca. 50 bit gegen regelbasierte kombinierte Brute-Forcing/Dictionary-Angriffe)*

Was macht *Forced Forcing© so sicher und einzigartig?*

- Ein Angreifer kann den gemerkten und den angehängten Passwortteil **nicht separat angreifen**
- Nur **zusammen** entsteht das **gültige Passwort**
- Das bedeutet: Ihre Stärken addieren sich nicht, sie **multiplizieren** sich
- Es ist keine neue Applikation, sondern eine code-basierende Methodik
- Könnte ein Angreifer mit einem absoluten High-End-System z. B. einem Hochleistungsrechner, Botnetz oder gar Quantencomputer ein Passwort ohne ***Forced Forcing***© innerhalb einer Stunde knacken, so braucht er nun für den gleichen Angriff einige **Millionen Stunden bzw. einige Jahrhunderte**
- Und das, ohne dass sich für den Anwender irgendetwas ändert – er verwendet das **gleiche Passwort** und muss nicht einmal wissen, dass es mit ***Forced Forcing***© geschützt ist
- Es erfordert null-Maintenance und produziert keinerlei technische Folgekosten
- Es ist binnen weniger Tage global einsatzfähig

Forced Forcing©

Cyberbreeze
Platanenweg 2
63303 Dreieich
Sven.Herrmann@join4business.com

Sven Herrmann, Thomas Wolf