Forced Forcing©

Genuine protection for all password & knowledge-based authentications

2022, Dreieich/Munich

cyberbreeze

Forced Forcing© in a nutshell

- **Password protection** will gain significant importance in the next few years due to the increasing number of remote applications and better technical attack options
- With ***Forced Forcing***© we have a unique, patented methodology to increase safety in potency
- ***Forced Forcing***© reduces all types password risks, is extremely secure, and cost-effective
- It is **installed** very quickly and, in contrast to many other applications and processes, does **not require any changes** at the user's and/or his customer's site
- We expect ***Forced Forcing***© to develop into a **global standard** in a short time

Through COVID-19 expect explosive growth of

- e-commerce
- Online- and Mobile-Banking
- Homeoffice, Home-Schooling and Education
- Digital authorities
- Video applications & conferencing services

New technologies and digital offerings require more security, such as

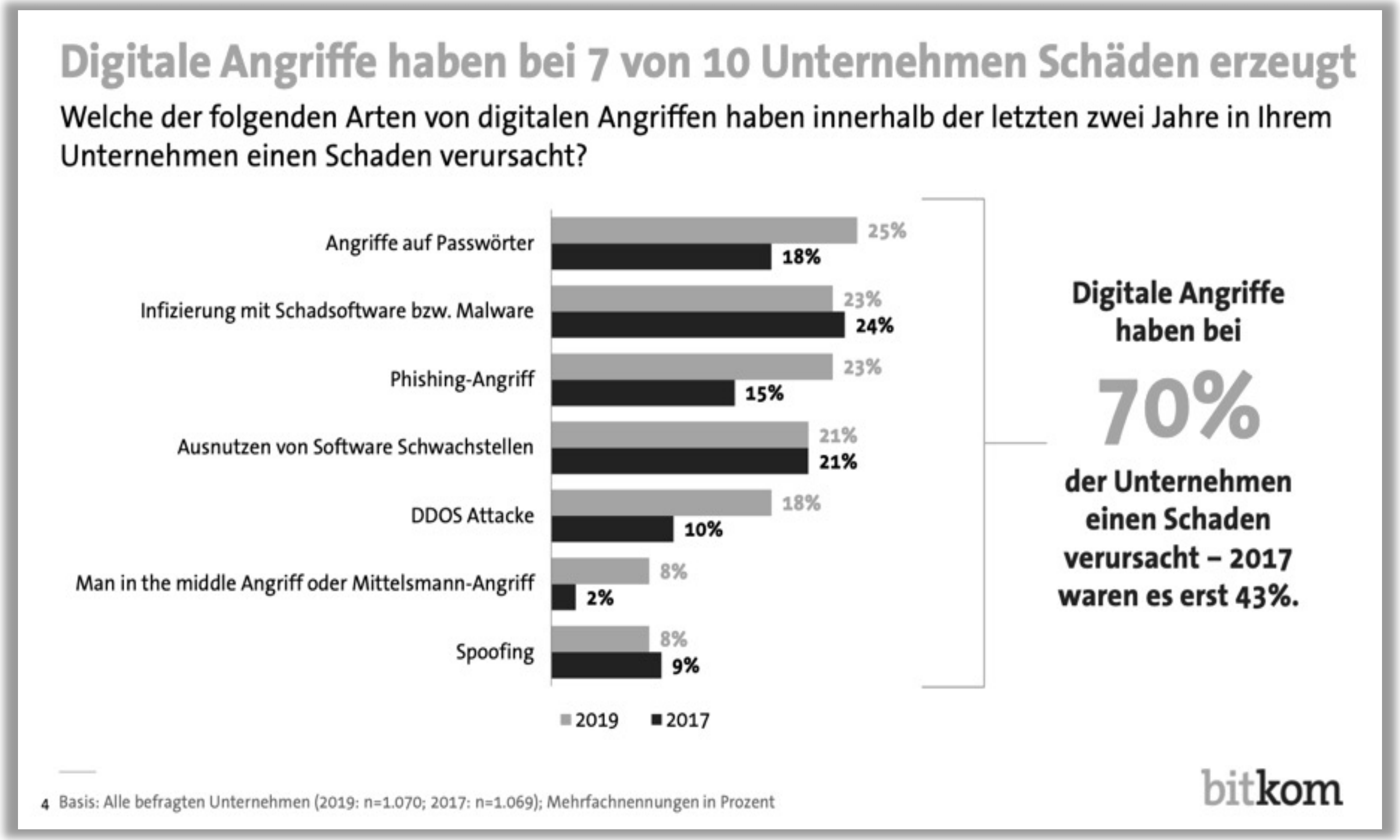
- Identity Management
- Digitization in Healthcare
- Blockchain, Krypto & open platform economics
- IoT/5G/Smarthome

Attention: : High-performance computers, quantum computers and bot-nets enable cyberattacks in a new dimension (think: bitcoin mining purpose-built computers)

Password
****

300 billion passwords worldwid means the No. 1 in authentication – and the trend is rising

Analyses confirm: The danger is growing!



Digitale Angriffe haben bei 7 von 10 Unternehmen Schäden erzeugt

Welche der folgenden Arten von digitalen Angriffen haben innerhalb der letzten zwei Jahre in Ihrem Unternehmen einen Schaden verursacht?

Digitale Angriffe haben bei

70%

der Unternehmen einen Schaden verursacht – 2017 waren es erst 43%.

4 Basis: Alle befragten Unternehmen (2019: n=1.070; 2017: n=1.069); Mehrfachnennungen in Prozent

bitkom

Damages of approx.
200 billion € in Germany
2019 only

All authentication methods have significant weaknesses

Method:	Valuation:
Knowledge Passwords, PIN, praphical elements or question-answer principle	**Insecure,** as the human brain is overwhelmed with the increasing demands of necessary complexity and quantity of passwords
Ownership Devices, smartcards, tokens	**Insecure**, because the property can be stolen, copied or hacked
Inherence Biometric feature	Very convenient but **insecure**, not changeable, can be recorded and can be copied using new technologies and methods

Risks from high-performance computers & quantum computing significantly increasing.

Increasing computing power now demands even more password protection

Brute Forcing: Trying out large sets of character combinations

Dictionary Attacks: Trying out common words, names and terms

Pattern / Combined Attacks: Structured search for patterns in combinations of letters, numbers and characters e.g. "H@nnover21".

Passwort Spray / Database Attack: Automated attempts of frequently used passwords like "Secret123!" for all users of a larger user base

Interface Attacks / Offline Attacks: Automated (through an interface) or offline (against a hash) attempts, in connection with the methods above, increasing attack speed dramatically. Also possible for password-protected encrypted files (e.g. ZIP files) or against hardware

Alternative Attack Vectors: The use of master passwords opens up a new attack vector for an attacker, namely the attack on the password administration itself: If they succeed, they have compromised all passwords - at once!

The solution: *Forced Forcing©*

Forced Forcing© = memory capability x computational power

Forced Forcing© =
Memory capability x computational power

- The **human-generated password** (or the human-generated information in the general case of knowledge-based authentication) is **supplemented by a second, randomly generated part**
- The user does **not have to remember this second part**, can ignore it completely and does not even have to know about its existence
- Instead, the user‘s **own computer system** is forced to determine its own password on the basis of the entered, memorized password part by means of forced brute forcing (hence, ***Forced Forcing©***) for every legitimate authentication
- The length as well as the complexity of the additional random part is chosen in such a way that it only moderately burdens the computing power of the user system (e.g. 1 second)
- In practice, this means today that a common cell phone or a simple notebook can and must try through **several million password possibilities** when performing the authentication
- So the user experience is **not** significantly **affected**, but **security is boosted** literally **exponentially**

Simplified password generation and combined authentication

1. **Password creation:**
   - The user generates and remembers his password, for instance: **sus@Nne42;**
   - The user's system generates an additional and completely random password from, for example, six numbers. This means that the user password in combination becomes more secure by a factor of 1 million : 738482
   - After generating the password hash, the randomly generated password component can be discarded; no storage is required
2. **Legitimization and Authentification:**
   - The user enters his password as usual: **sus@Nne42;**
   - With the help of brute forcing, the user's system finds the second - i.e. randomly generated and not stored component of the password : 000000 … 999999 -> 738482
   - The user's system authenticates to the target system with the combined password : **sus@Nne42;738482**

By combining the two password components, the security increases exponentially

Duration on the attack of:	Time for users	Time for attackers
Moderately strong password (common password rules/best practices) ***(memory capability)***	Not required	**Approx. 1 hour** **-> Feasible in practice**
Forced Forcing© *part* ***(computational power)***	**Approx. 1 second** („forced“)	Not possible since not separately attackable
New combined protection ***(memory capability x computational power)***	Not required	**Approx. 228 years** **-> Attack is no longer realistically feasible**

A pentest commissioned by an international insurance group proved the effectiveness of ***Forced Forcing ©***. An independent scientific institute will also examine and test it.

Assumptions:

- *Offline-Hash attack is possible (-> high speed of attack)*
- *Computational attacker power of 300 billions hashes/sec (e.g. 5 Amazon p3.16x large instances)*
- *Computational defender power of 2 Mio. hashes/sec (e.g. a mid-range smartphone)*
- *Moderately strong password according to common password rules (corresponds to resilience of approx. 50 bit against rule-based combined brute forcing/dictionary attacks)*

What makes *Forced Forcing*© so secure?

- An attacker **cannot attack** the remembered and the appended **password parts separately**
- Only **together** the **valid password** is created
- This means: Their strengths do not simply add up, they **multiply**
- Hence “**memory capability x computing power**“
- As a consequence: If an attacker with an extreme high-end system, e.g., a high-performance computational instance, botnet, or even quantum computer could crack a password without ***Forced Forcing***© within 1 hour, he would now **need several million hours (i.e. several centuries)** for the same attack.
- And finally: Without changing anything for the user - they use the same password and do not even have to know that it is protected with ***Forced Forcing***© now.

Let‘s establish *Forced Forcing*© together as a leading global security standard!

Cyberbreeze
Platanenweg 2
63303 Dreieich, Germany
info@cyberbreeze.io

Sven Herrmann