Universitätsmedizin Essen
Universitätsklinikum

# UK-Essen
## - Passwörter & Verschlüsselung -

**Frank Lorenz (ISB)**

# Passwort – Warum ist die Länge entscheidend?

| Passwortlänge in Zeichen | Genutzte Zeichen | Dauer |
|---|---|---|
| 5 | Kleinbuchstaben (26 mögliche Zeichen) | 0,069 Sekunden |
| | Klein- & Großbuchstaben & Ziffern (62 mögliche Zeichen) | 5,4 Sekunden |
| | Klein- & Großbuchstaben, Ziffern & Sonderzeichen (95 mögliche Zeichen) | 45,4 Sekunden |
| 6 | Kleinbuchstaben (26 mögliche Zeichen) | 1,8 Sekunden |
| | Klein- & Großbuchstaben & Ziffern (62 mögliche Zeichen) | 5 Minuten 30 Sekunden |
| | Klein- & Großbuchstaben, Ziffern & Sonderzeichen (95 mögliche Zeichen) | 1 Stunde 48 Minuten |
| 7 | Kleinbuchstaben (26 mögliche Zeichen) | 47,1 Sekunden |
| | Klein- & Großbuchstaben & Ziffern (62 mögliche Zeichen) | 5 Stunden 42 Minuten |
| | Klein- & Großbuchstaben, Ziffern & Sonderzeichen (95 mögliche Zeichen) | 4 Tage 17 Stunden |
| 8 | Kleinbuchstaben (26 mögliche Zeichen) | 20 Minuten 24 Sekunden |
| | Klein- & Großbuchstaben & Ziffern (62 mögliche Zeichen) | 14 Tage 19 Stunden |
| | Klein- & Großbuchstaben, Ziffern & Sonderzeichen (95 mögliche Zeichen) | 1 Jahr 2 Monate 12 Tage |

Basis hierfür ist eine mögliche Erstellung von 170.424.973 Keys (mögliche Passwörter) pro Sekunde

# Passwort – Mögliche Angriffsformen

## Wörterbuchangriff

Diese Angriffsmethode macht sich zunutze, dass Passwörter oft zu kurz sind oder geläufige Wörter enthalten. Hacker nutzen eine Liste mit solchen Wörtern (das „Wörterbuch“) und probieren sie zumeist in Kombination mit einigen Ziffern vor und/oder nach den Benutzernamen des Unternehmens aus. (Die Benutzernamen sind leicht herausfindbar, da sie in der Regel auf den Namen der Mitarbeiter basieren.)

## Brute Force

Mithilfe eines Programms werden wahrscheinliche Passwörter oder einfach zufällige Zeichenketten erzeugt und quasi nach der Holzhammermethode ausprobiert. Der Angriff beginnt mit häufig genutzten, schwachen Passwörtern wie Passwort123 und steigert sich dann. Auch Variationen mit Groß- und Kleinbuchstaben werden automatisch durchprobiert.

## Abgefangene Daten

Bei dieser Angriffsmethode nutzen die Cyberkriminellen Sniffer-Software, um den Datenverkehr im Netz zu überwachen und Passwörter bei der Übertragung abzufangen. Ähnlich wie beim Abhören einer Telefonleitung erlangt die Software die gesuchten Informationen also einfach per Lauschangriff. Sind diese Informationen (z. B. die Passwörter) unverschlüsselt, wird die Aufgabe umso leichter. Aber auch verschlüsselte Informationen können anfällig sein, je nach Stärke des genutzten Verschlüsselungsverfahrens.

# Passwort – Mögliche Angriffsformen

## "Man-in-the-Middle"

Die Software des Hackers überwacht nicht einfach nur die im Netz übertragenen Daten, sondern schaltet sich aktiv in die Interaktion mit dem Benutzer ein. Dazu tarnt sie sich meist als seriöse Website oder App, um so den Benutzer zur Eingabe seiner Zugangsdaten und anderer vertraulicher Informationen (Kontonummern, Sozialversicherungsnummern usw.) zu bewegen. Dieser sogenannte "Man-in-the-Middle-" (MITM) oder Janusangriff wird oft mittels Social Engineering realisiert (der Benutzer wird durch Vortäuschung falscher Tatsachen in die Irre geführt).

## Keylogger

Cyberkriminelle installieren Software auf dem System des Benutzers, die jede Tastatureingabe protokolliert. So finden die Ganoven nicht nur den Benutzernamen und das Passwort heraus, sondern sie erfahren auch gleich, für welche Website oder App die Zugangsdaten jeweils gelten. Bei dieser Angriffsart ist in der Regel ein vorhergehender Angriff nötig, bei dem die Keylogger-Schadsoftware auf dem Computer des Benutzers installiert wird.

# Passwort – Mögliche Angriffsformen

## Social Engineering

Social Engineering umfasst eine Reihe von manipulativen Methoden, mit denen Benutzern vertrauliche Informationen entlockt werden. Zu den gängigen Taktiken zählen:

***Phishing:*** Betrügerische E-Mails, SMS usw. sollen Benutzer dazu bringen, ihre Zugangsdaten einzugeben, gefälschte Websites aufzurufen oder auf einen Link zu klicken, der die Installation von Schadsoftware auslöst.

***Spear Phishing:*** Vergleichbar mit Phishing, allerdings sind die E-Mails/SMS hier sorgfältiger formuliert und mithilfe von bereits herausgefundenen Informationen stärker auf den jeweiligen Benutzer zugeschnitten. Wenn der Hacker zum Beispiel schon weiß, dass sein Opfer ein Konto bei einer bestimmten Bank hat, kann er Layout und Logo der E-Mail im Stil der Bank gestalten, um authentischer zu wirken.

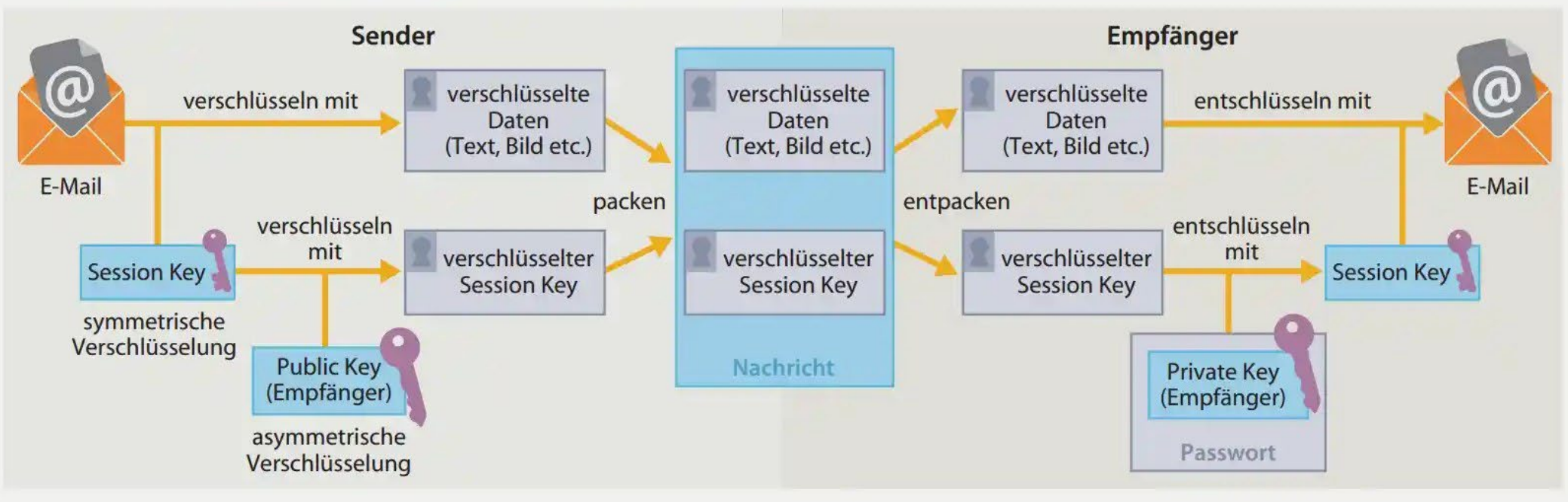
***Baiting:*** Angreifer hinterlassen kompromittierte USB-Sticks oder andere Geräte an öffentlichen Plätzen oder im Unternehmen in der Hoffnung, dass Mitarbeiter sie ahnungslos benutzen und so auch ihre Computer infizieren.

***Quid pro quo:*** Der Angreifer gibt sich als vertrauenswürdige Person aus, zum Beispiel als Helpdesk-Mitarbeiter, und interagiert mit dem Benutzer, um von ihm die gewünschten Informationen zu erhalten.

# Passwort – Excel-Tabelle

# Verschlüsselung – Was ist das?

# Verschlüsselung – Wie geht das?



# Signieren – Was ist das?