IT-Sicherheit: Unterwegs zwischen zwei Welten
Technik, Menschen, Management & Führung

Jens Liebchen - RedTeam Pentesting GmbH
jens.liebchen@redteam-pentesting.de
https://www.redteam-pentesting.de

Aachen, 21. Oktober 2021

Über den Vortrag

Agenda:

- ★ Verschiedene Bereiche der IT-Sicherheit
- ★ Kombiniert mit Aspekten aus der Managementtheorie
- ★ Ziel: Technische Aspekte verstehen, richtige Entscheidungen treffen

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004 in Aachen
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Weltweite Durchführung von Penetrationstests
- ★ Forschung im Bereich der IT-Sicherheit

Datensicherheit

Woran denken Sie, wenn Sie an Datensicherheit denken?

Passwörter

Passwörter

- Nicht schon wieder...
- Ein Angreifer sucht immer die schwächste Stelle
- Was ist einfacher, als ein Passwort auszuprobieren oder zu erraten?

Passwörter

Passwörter

- ★ Nicht schon wieder...
- ★ Ein Angreifer sucht immer die schwächste Stelle
- ★ Was ist einfacher, als ein Passwort auszuprobieren oder zu erraten?

Verteidigung

Typische Verteidigung:

- ★ Keine (ausschließliche) Verwendung von Passwörtern
- ★ Passwort-Policies erzwingen „komplexe“ Passwörter
- ★ Account-Sperre nach zu vielen Fehleingaben

Beispiel: Passwort-Policy

Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

Beispiel: Passwort-Policy

Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2021_1`

Beispiel: Passwort-Policy

Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2021_2`

Beispiel: Passwort-Policy

Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2021_3`

Beispiel: Passwort-Policy

Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2021_4`

Beispiel: Passwort-Policy

Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2022_1`

Beispiel: Passwort-Policy

Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

$\Rightarrow$ `Pass2022_2`

Passwort-Policy

„Diese blöden Benutzer umgehen unsere Policy!“

Exkurs: Changes/Veränderungen

Changes/Veränderungen

Changes sind negativ.

- Menschen reagieren tendenziell negativ auf Veränderungen
- Extern ausgelöste Veränderungen, die Menschen direkt oder indirekt betreffen, werden als Angriff gewertet
- Selbst in positiven Veränderungen werden negative Begründungen gesucht

Exkurs: Changes/Veränderungen

Changes/Veränderungen

Changes sind negativ.

- ★ Menschen reagieren tendenziell negativ auf Veränderungen
- ★ Extern ausgelöste Veränderungen, die Menschen direkt oder indirekt betreffen, werden als Angriff gewertet
- ★ Selbst in positiven Veränderungen werden negative Begründungen gesucht

Exkurs Changes: Mitarbeiterführung

Kommunikation Chef ⇒ Mitarbeiter

„Herr Maier, ab heute bekommen Sie pro Monat 500 Euro mehr.“

- Eindeutig positive Aussage
- Aber Gedanken von Herrn Maier:
  - Erwartet mein Chef, dass ich jetzt mehr/schneller/länger arbeite?
  - Haben andere gute Mitarbeiter etwa gekündigt und ich soll (auf dem sinkenden Schiff) gehalten werden?
  - Bekommen alle anderen etwa auch mehr Geld?
  - ...

Exkurs Changes: Mitarbeiterführung

Kommunikation Chef ⇒ Mitarbeiter

„Herr Maier, ab heute bekommen Sie pro Monat 500 Euro mehr.“

- ★ Eindeutig positive Aussage
- ★ Aber Gedanken von Herrn Maier:
  - ★ Erwartet mein Chef, dass ich jetzt mehr/schneller/länger arbeite?
  - ★ Haben andere gute Mitarbeiter etwa gekündigt und ich soll (auf dem sinkenden Schiff) gehalten werden?
  - ★ Bekommen alle anderen etwa auch mehr Geld?
  - ...

Exkurs Changes: Mitarbeiterführung

Kommunikation Chef ⇒ Mitarbeiter

„Herr Maier, ab heute bekommen Sie pro Monat 500 Euro mehr.“

- ★ Eindeutig positive Aussage
- ★ Aber Gedanken von Herrn Maier:
  - ★ Erwartet mein Chef, dass ich jetzt mehr/schneller/länger arbeite?
  - ★ Haben andere gute Mitarbeiter etwa gekündigt und ich soll (auf dem sinkenden Schiff) gehalten werden?
  - ★ Bekommen alle anderen etwa auch mehr Geld?

  ...

Passwort-Policy

Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

- ★ Passwort-Policy ist nichts anderes als ein Change
- ★ Einmalig definiert, aber alle drei Monate wirkend
- ★ Mitarbeiter fühlen sich gegängelt
- ★ „Als ob jemand mein Passwort raten könnte...“
- ★ Kein Verständnis, stattdessen mehr oder weniger kreative Umgehung

Passwort-Policy

Passwort-Policy

„Ihr Kennwort ist mindestens 10 Zeichen lang, wobei mindestens ein Großbuchstabe, eine Ziffer und ein Sonderzeichen enthalten ist. Das Passwort muss alle 3 Monate gewechselt werden.“

- ★ Passwort-Policy ist nichts anderes als ein Change
- ★ Einmalig definiert, aber alle drei Monate wirkend
- ★ Mitarbeiter fühlen sich gegängelt
- ★ „Als ob jemand mein Passwort raten könnte...“
- ★ Kein Verständnis, stattdessen mehr oder weniger kreative Umgehung

Sperrung des Zugangs bei zu vielen Fehleingaben

- „Wenn ein Angreifer nur fünf Versuche hat, kann mein Passwort nie erraten werden...“
- „Wenn ein Angreifer nur fünf Versuche hat, braucht mein Passwort gar nicht mehr komplex zu sein...“
- „Niemand nutzt ein so einfach zu erratenes Passwort...“
- Angreifer: Wetten doch?

Ein magisches Passwort

FIRMENNAME123!

Passwortraten

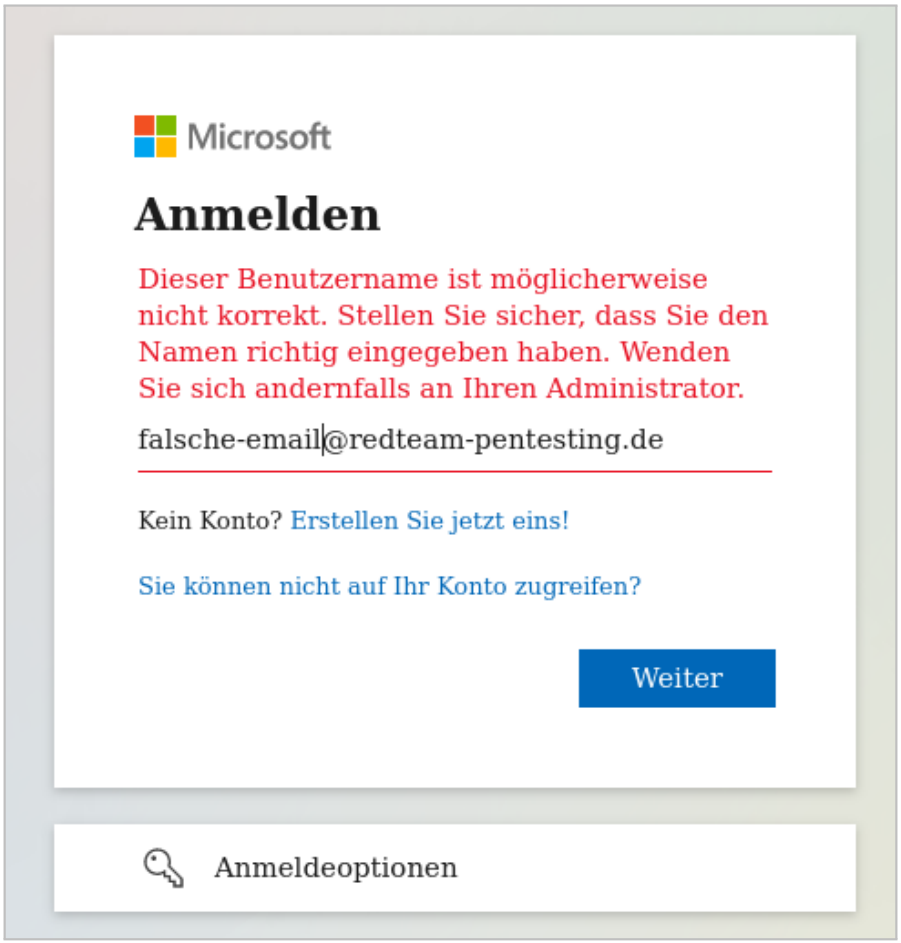
- Viele Passwörter/Benutzer ausprobieren ⇒ Account-Sperre
- Ein Passwort für viele Benutzer ausprobieren ⇒ keine Sperrung
- Woher kennt ein Angreifer die Benutzernamen?

Passwortraten

Woher kennt ein Angreifer die Benutzernamen?

- z.B. von Microsoft (`https://o365blog.com/post/desktopsso/`)

Passwortraten



Passwortraten

Woher kennt ein Angreifer die Benutzernamen?

- ★ z.B. von Microsoft (`https://o365blog.com/post/desktopsso/`)
- ★ klassische Username-Enumeration
- ★ andere Quellen: E-Mails oder erkennbares Muster

Passwörter, aber sicher?

- ★ Keine Passwortrotation ohne Anlass
- ★ Zettel am Bildschirm kann sicherer sein als schlechtes Passwort
- ★ Passwortmanager helfen gegen Vielzahl von gleichen oder unsicheren Passwörter
- ★ Diceware: `ZugUnfallTischTankstellenLaptopWindkraft`

Grundlagen: Password-Hashing

Wie speichert und kontrolliert ein Computer i.A. Passwörter?

- ★ Einwegfunktionen (Hashing)
- ★ Passwort $\Rightarrow$ Hash
- ★ Eingegebenes Passwort $\Rightarrow$ Hash $\Rightarrow$ Vergleich mit gespeichertem Hash

Windows-Hashes

```
RedTeam:501:
 742610767ed2afa4fd47512fa194174f:
 3c04e5a9b3e53249b257de8223118a45
```

Windows-Hashes

```
RedTeam:501:
 742610767ed2afa4fd47512fa194174f:
 3c04e5a9b3e53249b257de8223118a45
```
⇐ NT-Hash

Windows-Hashes

```
RedTeam:501:
 742610767ed2afa4fd47512fa194174f: ⇐ LM-Hash
 3c04e5a9b3e53249b257de8223118a45
```

LAN-Manager-Hashes

- Aus der Zeit vor Windows Vista!

LAN-Manager-Hashes

- ★ Aus der Zeit vor Windows Vista!
- ★ Keine Kleinbuchstaben

LAN-Manager-Hashes

- ★ Aus der Zeit vor Windows Vista!
- ★ Keine Kleinbuchstaben
- ★ Nur maximal 14 Zeichen

LAN-Manager-Hashes

- ★ Aus der Zeit vor Windows Vista!
- ★ Keine Kleinbuchstaben
- ★ Nur maximal ~~14~~ $2 * 7$ Zeichen

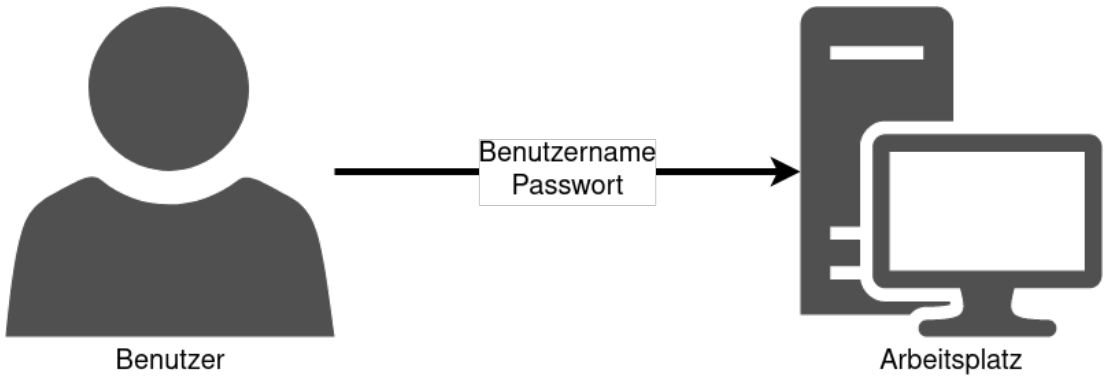
LAN-Manager-Hashes

- ★ Aus der Zeit vor Windows Vista!
- ★ Keine Kleinbuchstaben
- ★ Nur maximal ~~14~~ $2 * 7$ Zeichen
- ★ Aber selbst heute noch in fast jedem großen Netzwerk zu finden

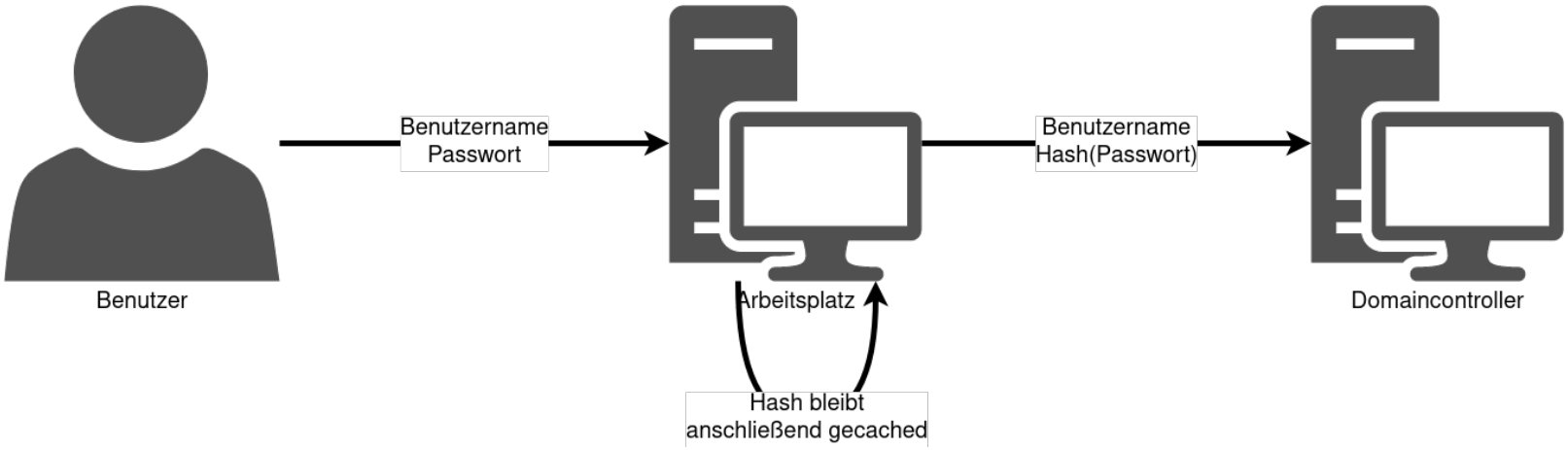
LAN-Manager-Hashes

- ★ Aus der Zeit vor Windows Vista!
- ★ Keine Kleinbuchstaben
- ★ Nur maximal ~~14~~ $2 * 7$ Zeichen
- ★ Aber selbst heute noch in fast jedem großen Netzwerk zu finden
- ★ Grafikkarten finden Passwort in wenigen Minuten

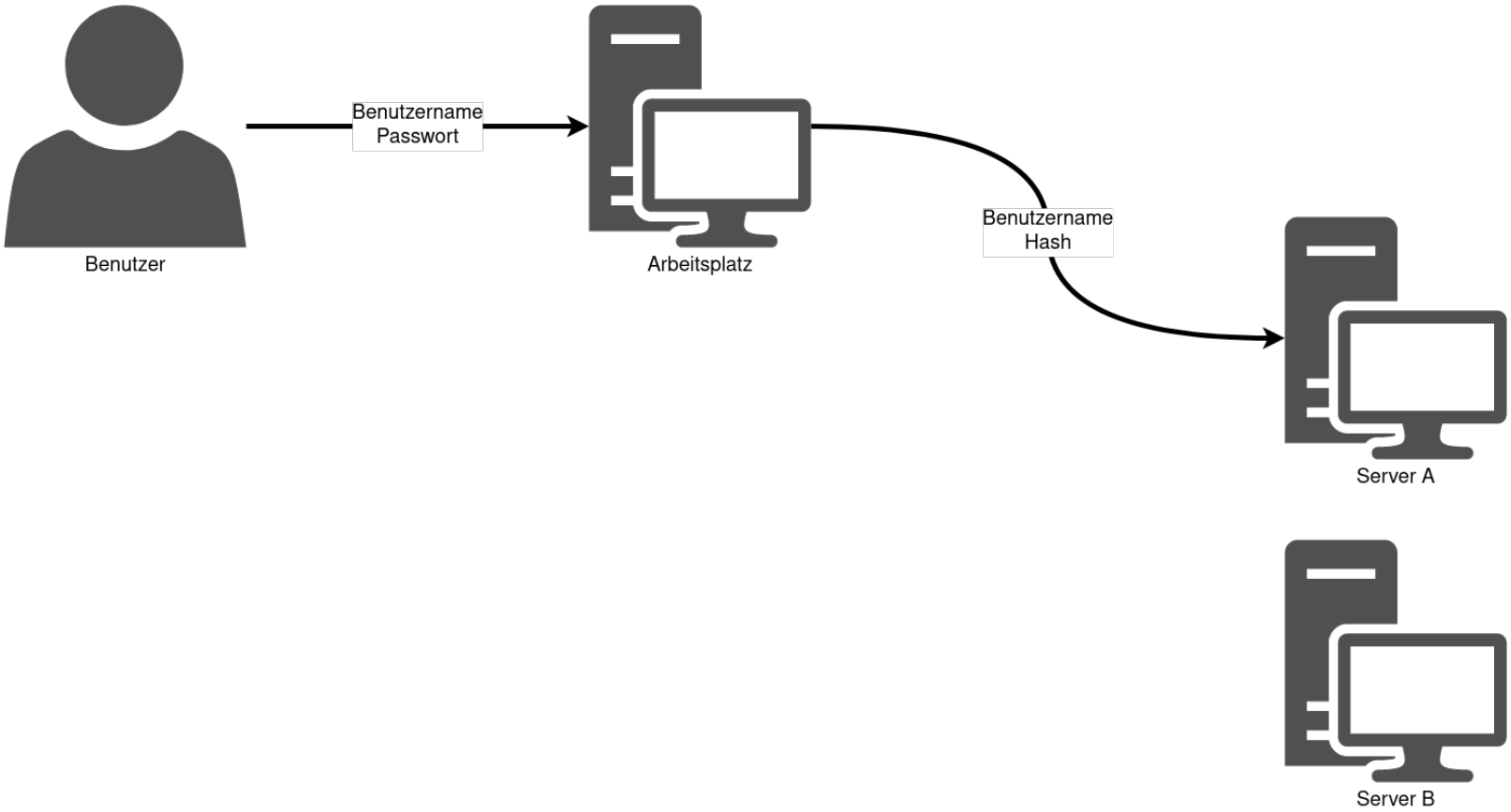
Windows Anmeldung (vereinfacht):



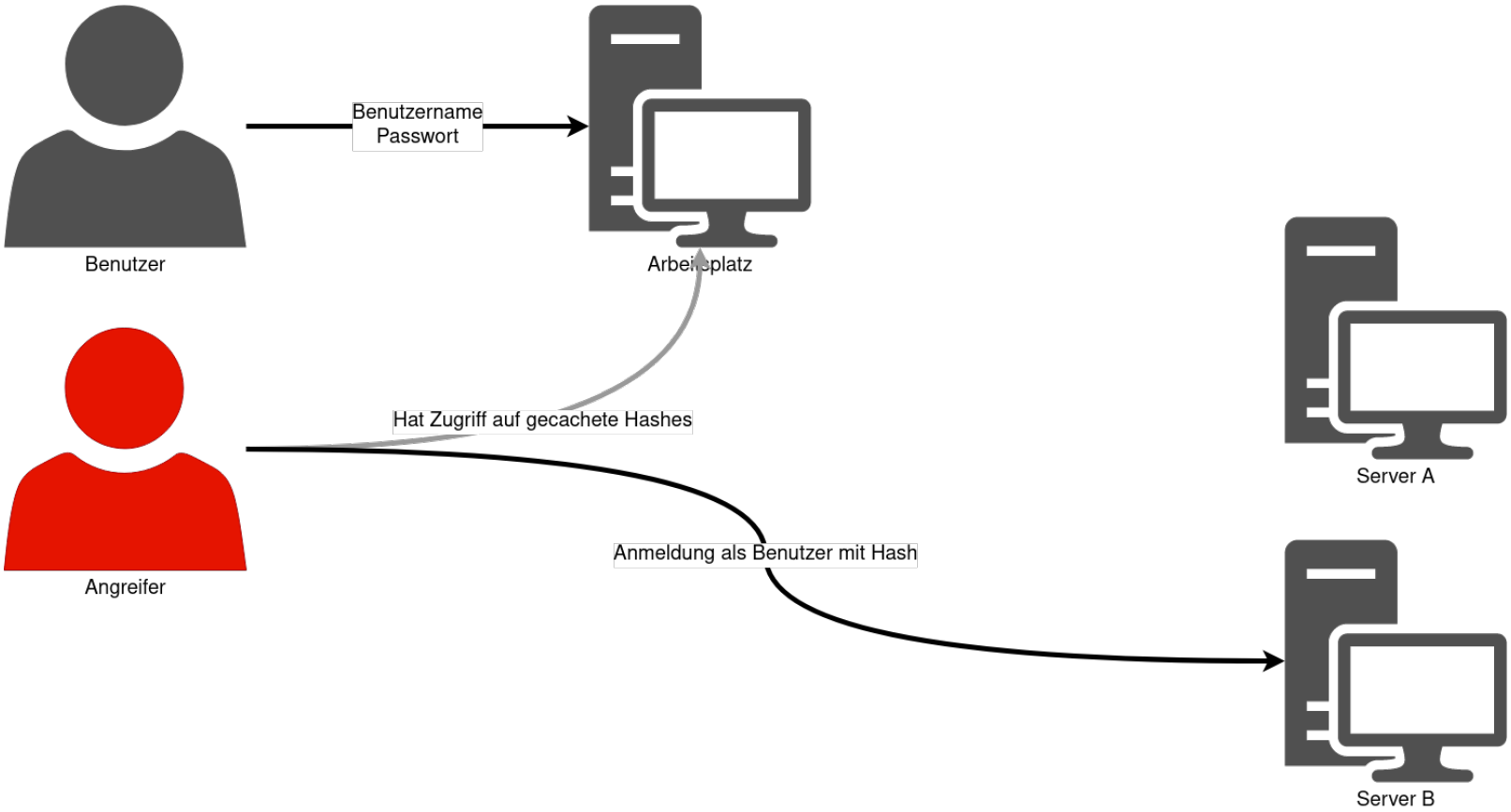
Windows Anmeldung (vereinfacht):



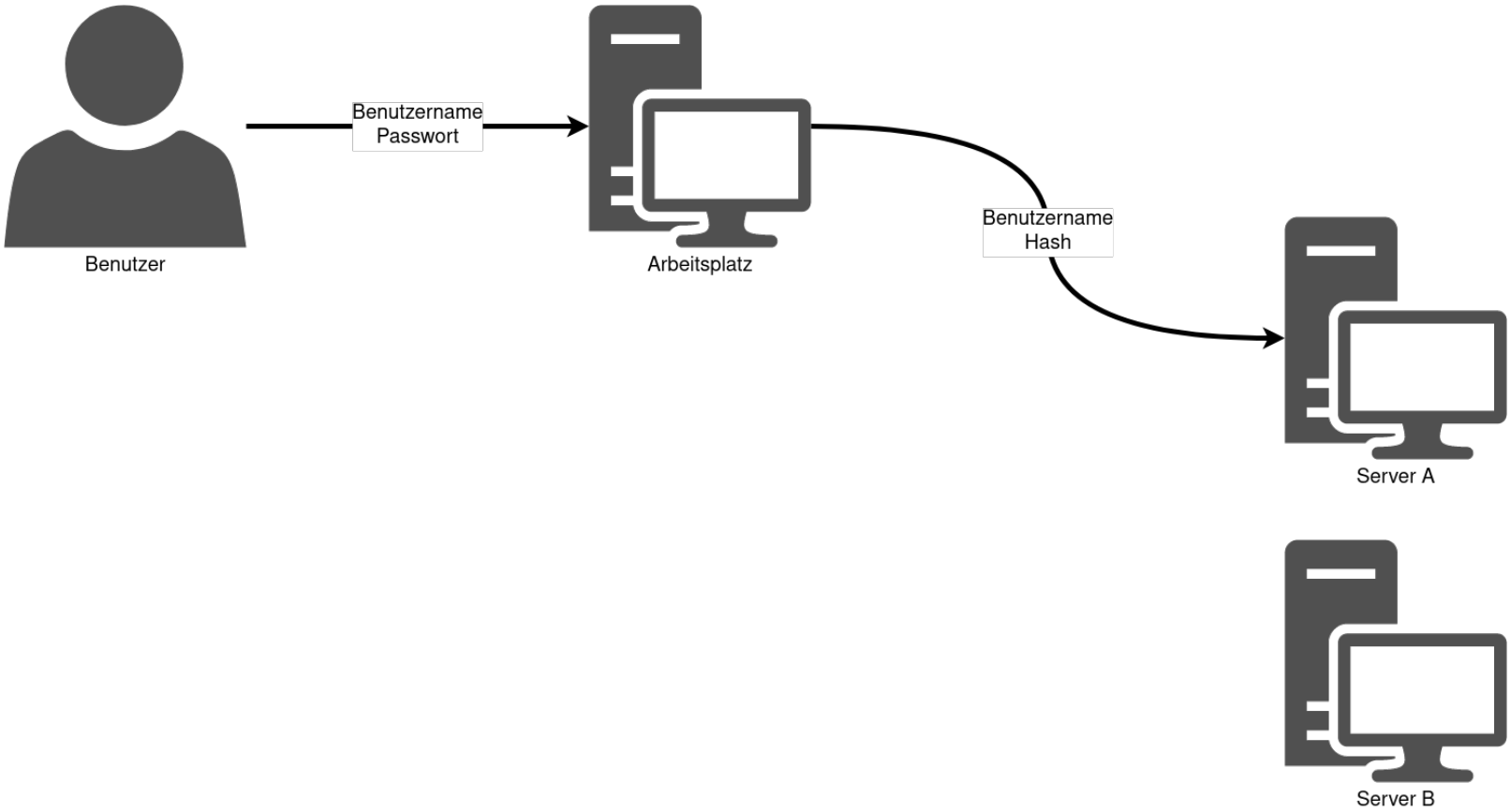
Windows Anmeldung (vereinfacht):



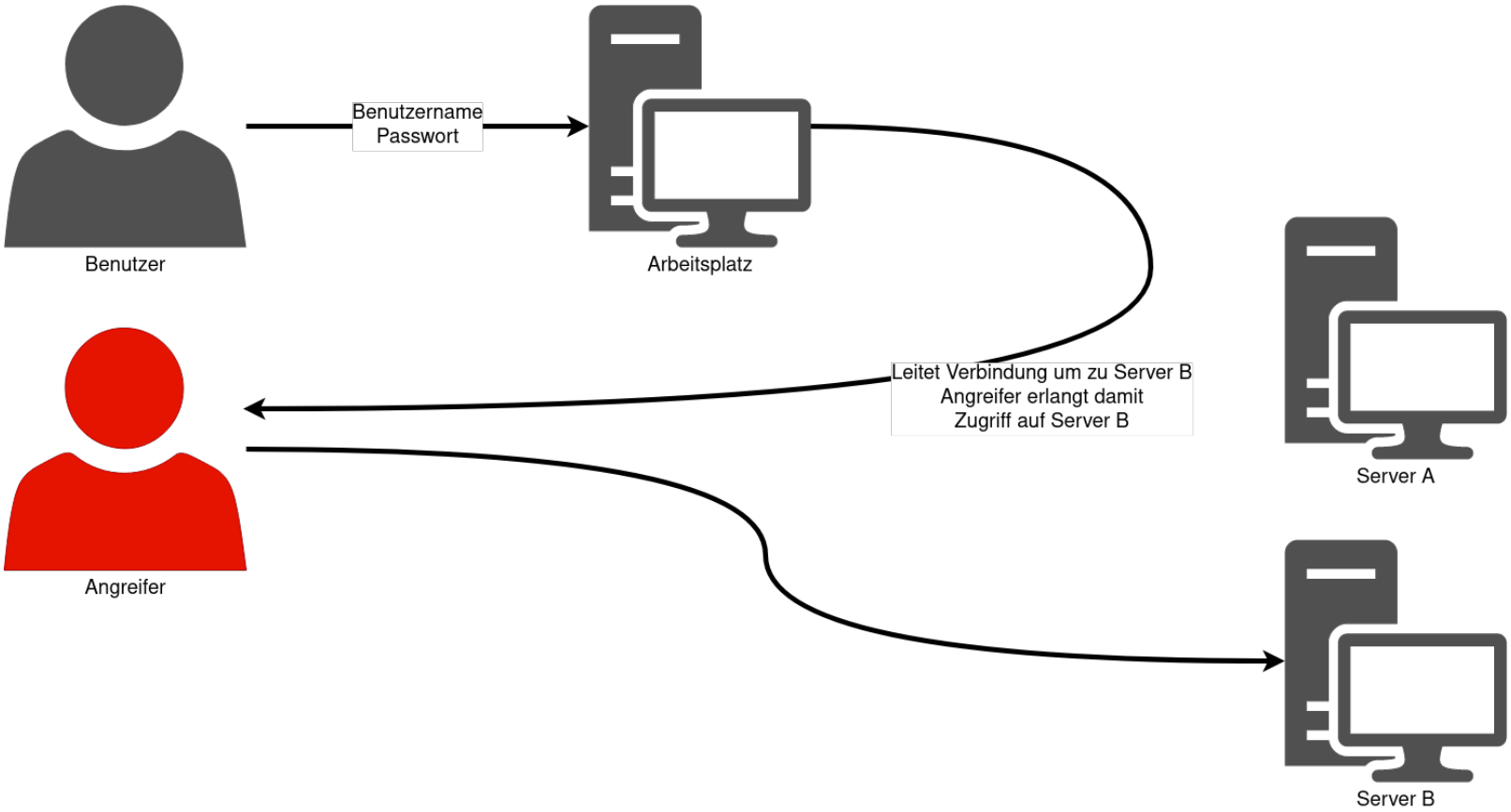
Windows Hashes & Angreifer (vereinfacht):



Windows Anmeldung am Server (vereinfacht):



Windows Angreifer im Netzwerk (vereinfacht):



Sicheres (mobiles) Arbeiten

Sicheres (mobiles) Arbeiten

Sicheres (mobiles) Arbeiten

- Verschlüsselung der Festplatte gegen Diebstahl des Geräts
- Gerät nicht ohne Aufsicht lassen (auch nicht ausgeschaltet)
  - Warum, ist doch verschlüsselt?

„Evil-Maid-Angriffe“

„Evil-Maid-Angriffe“

„Evil-Maid-Angriffe“

- ★ Angreifer greift zweimal zu
- ★ Beim ersten Angriff wird Gerät lediglich unbemerkt manipuliert
- ★ Manipulation ermöglicht z.B. das Speichern von Tastatureingaben
- ★ Erst beim zweiten Angriff wird Gerät gestohlen
- ★ $\Rightarrow$ Tastatureingaben zusammen mit Gerät ermöglicht Anmeldung und Entschlüsselung der Daten

Crypto-Trojaner (und andere unerwünschte Software)

Was ist (im ersten Schritt) passiert?

- ★ Ein Angreifer hat beliebigen Programmcode auf Ihrem Rechner ausgeführt
- ★ Diesen Angriff haben Sie bemerkt...

Was ist (im ersten Schritt) passiert?

- ★ Ein Angreifer hat beliebigen Programmcode auf Ihrem Rechner ausgeführt
- ★ Diesen Angriff haben Sie bemerkt...
- ★ ... leider aber nur, weil der Angreifer es so wollte!

⇒ Andere Angriffe bemerken Sie normalerweise nicht so einfach!

Crypto-Trojaner (und andere unerwünschte Software)

„Law 1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore."

(10 Immutable Laws of Security, Microsoft)

Und im Homeoffice?

- ★ Zutrittskontrolle?
- ★ Gefährden andere Netzwerkteilnehmer wie veraltete Geräte das sichere Firmennetzwerk?
- ★ Welche zusätzliche Videokonferenzsoftware gefährdet nun das Firmennetzwerk?
- ★ Gibt es privat und geschäftliche genutzte Geräte? Was ist mit Druckern?
- ★ Wie sieht es mit der Datenvernichtung von z.B. Ausdrucken im Homeoffice aus?

Und im Homeoffice?

- ★ Es bleiben die gleichen Angriffe...
- ★ ...nur kommen durch das Homeoffice neue dazu.

⇒ Erste Firmennetzwerke wurden in Penetrationstests erfolgreich über Homeoffice-Komponenten angegriffen!

Und jetzt?

Und jetzt?

Exkurs: Binäres Denken

Binäres Denken

Menschen tendieren dazu, nur schwarz-weiß zu denken.

Exkurs: Binäres Denken

Binäres Denken

Menschen tendieren dazu, nur schwarz-weiß zu denken.

- „Ich vertraue meinen Kollegen, warum soll da noch über Zugriffskontrolle gesprochen werden?“
- „Ich brauche die Software X, da kann man halt nichts machen...“

Exkurs: Binäres Denken

Binäres Denken

Menschen tendieren dazu, nur schwarz-weiß zu denken.

- „Ich vertraue meinen Kollegen, warum soll da noch über Zugriffskontrolle gesprochen werden?“
- „Ich brauche die Software X, da kann man halt nichts machen...“
- Nach Snowden-Veröffentlichungen:
  - Resignation („Jetzt ergibt ja alles keinen Sinn mehr.“)
  - Aktionismus („Wir müssen uns vor der NSA schützen!“)

Binäres Denken

- ★ Binäres Denken blockiert lösungsorientiertes Handeln
- ★ 100%-Lösungen existieren nicht
- ★ Resignation und Aktionismus gefährdet Unternehmensfortbestand

Exkurs: Managementtheorie

„Führen heißt entscheiden“

(Michael Löher, Führung neu denken)

Exkurs: Managementtheorie

- ★ Entscheidungen finden auf allen Ebenen statt
- ★ Je höher die Ebene, desto mehr Entscheidungen unter Unsicherheiten
- ★ Nicht entscheiden ist schlechter als falsch entscheiden!

Exkurs: Managementtheorie

- ★ Entscheidungen finden auf allen Ebenen statt
- ★ Je höher die Ebene, desto mehr Entscheidungen unter Unsicherheiten
- ★ Nicht entscheiden ist schlechter als falsch entscheiden!
- ★ IT-Sicherheit ist dabei keine Ausnahme!

Binäres Denken

Treffen Sie adäquate Entscheidungen!

Wie Sie es Angreifern besonders einfach machen...

- ★ Spielen Sie Updates nicht ein! („Never change a running system!“)

Wie Sie es Angreifern besonders einfach machen...

- ★ Spielen Sie Updates nicht ein! („Never change a running system!“)
- ★ Nutzen Sie veraltete Systeme!

Wie Sie es Angreifern besonders einfach machen...

- ★ Spielen Sie Updates nicht ein! („Never change a running system!“)
- ★ Nutzen Sie veraltete Systeme!
- ★ Ändern Sie keine Standardpasswörter oder lassen Sie die Passwörter gleich weg!

Wie Sie es Angreifern besonders einfach machen...

- ★ Spielen Sie Updates nicht ein! („Never change a running system!“)
- ★ Nutzen Sie veraltete Systeme!
- ★ Ändern Sie keine Standardpasswörter oder lassen Sie die Passwörter gleich weg!
- ★ Kümmern Sie sich später um IT-Sicherheit, wenn Zeit dafür da ist!

Fazit

- ★ Angriffe finden statt
- ★ Auch/Gerade bei kleineren Unternehmen
- ★ Treffen Sie adäquate Entscheidungen zur IT-Sicherheit...
- ★ ...und setzten Sie die richtigen Prioritäten bei Ihren Entscheidungen!

Zeit für Fragen und Diskussionen

Vielen Dank für Ihre Aufmerksamkeit!

In Kooperation mit:

Stadtmarken