



Gesundheit für ihre IT.®



30. MAI 2017 | 14.00 – 19.00 UHR, WEIDMÜLLER GMBH IZ NÖ SÜD, STRASSE 2B, OBJ. M59 | 2355 WIENER NEUDORF



DIGITALISIERUNG | ROBOTISIERUNG | INDUSTRIE 4.0 | IT

Schutz vor Cybercrime

IT-Security – ein Erfahrungsbericht

ZT DI Dr.tech.

Wolfgang Prentner, ZTP

Informatiker und gelernter Mechaniker

INHALTSVERZEICHNIS

1. Einleitung
2. Zahlen und Fakten
3. 5 Alltagsgeschichten
4. Wie schütze ich mein Unternehmen?
5. Zusammenfassung



Einleitung

ZTP_{.AT}

ZT WOLFGANG PRENTNER

1. Gründung 1998
2. Promotion in IT-Security
3. 25 Jahre Berufserfahrung
4. 12 Mitarbeiter
5. Umsatz ca. €1.5 Mio. 2016



DIENSTLEISTUNG

**Gibt Hackern
keine Chance!**

INTERNET SICHERHEITSGURT[®].at

CyberSecurity prüfen . zertifizieren . haften

Unabhängige

Prüfstelle für Informatik . CyberSecurity & Datenschutz

Gesundheit für Ihre IT.

ZfP 
IT-Zivildienst . staatlich besidet

VORGEHENSWEISE

Die Sicherheitsformel zum Datenschutz



Geprüfte Web-Sicherheit mit staatlich anerkanntem Zertifikat.
Wir prüfen Websysteme mit mächtigen Scan-Werkzeugen und gezielten Hacking-Angriffen.
Nach der Zertifizierung haften wir mit mind. *1,5 Mio. Euro für die Sicherheit der geprüften Systeme.
*abhängig von der Vertragsgestaltung



Kontaktieren Sie uns!

ZTP Prentner IT GmbH, Ziviltechnik-Gesellschaft für Informations- & Kommunikations-Technologie, Wien, NÖ, Vorarlberg, Tel. +43-1-532 46 86 Fax-DW-20, Mail: office@ztp.at www.ztp.at



Kennen Sie Ihre eigenen
Computersysteme oder
Netzwerke?

2

0010

ZAHLEN UND FAKTEN

Digitale Angriffe treffen jedes zweite Unternehmen

Anteil Unternehmen, die in den letzten 2 Jahren von Datendiebstahl, digitaler Wirtschaftsspionage oder Sabotage betroffen waren





51 Milliarden Euro
Schaden pro Jahr

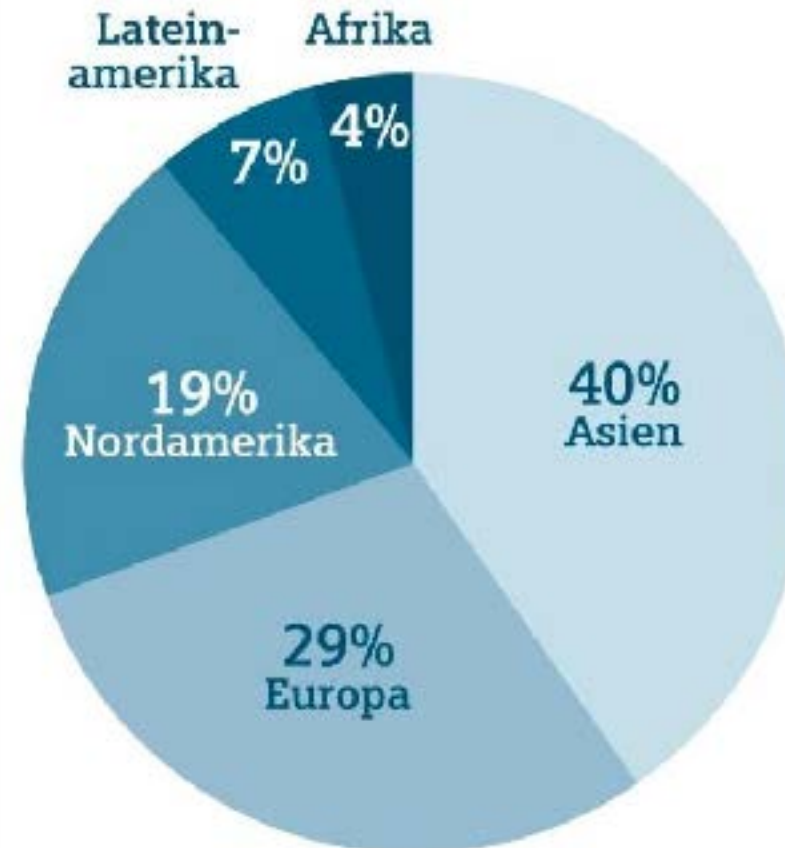


INDUSTRIE 4.0

M2M MARKTANTEILE

Kommunikation von Maschine zu Maschine: Asien klar an der Spitze

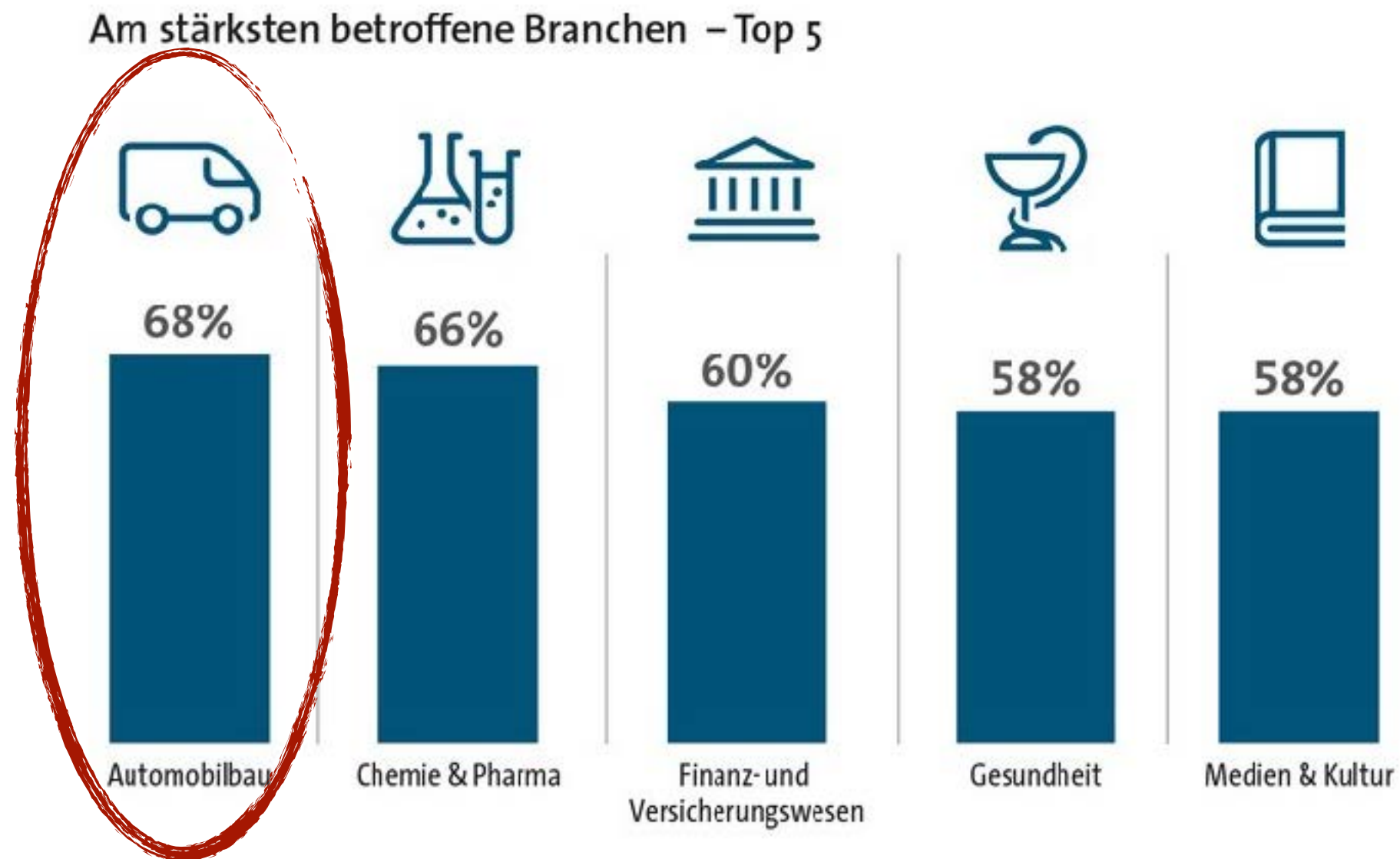
Weltweite Anteile am M2M-Markt
(2013)



Quelle: GSMA

CYBER-ANGRIFFE

BETROFFENE BRANCHEN



SCHAD.PROGRAMM.VARIANTEN (JÄHRLICH)

JÄHRLICHER ANSTIEG BEKANNTER SCHADPROGRAMM VARIANTEN



Quelle: AV-Test

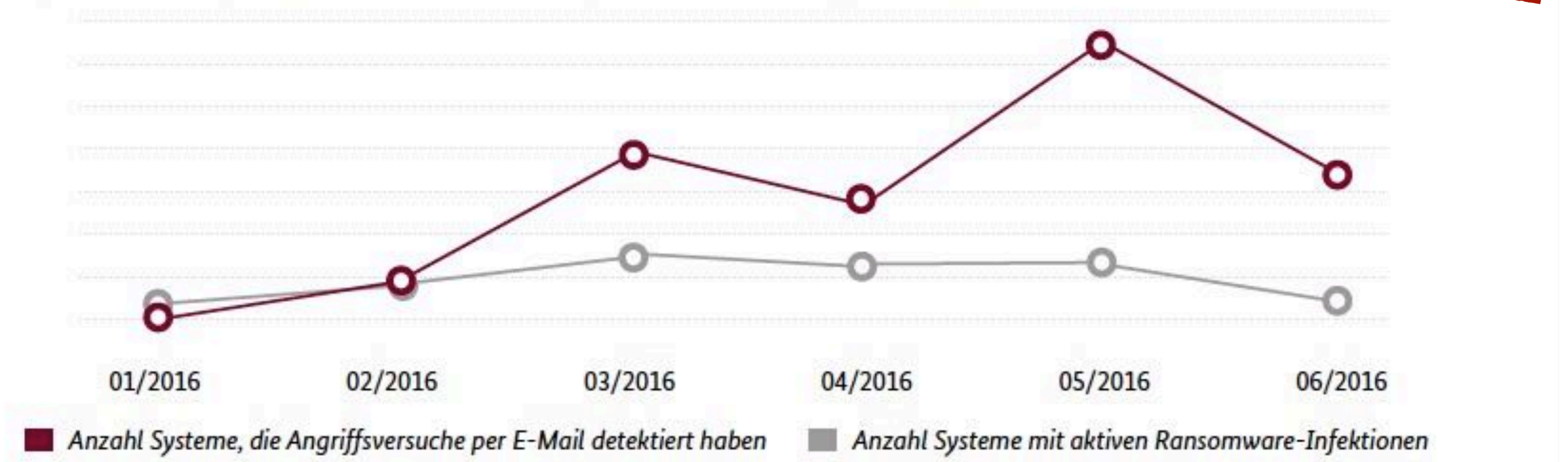
ERPRESSER.SCHAD.SOFTWARE

(RANSOMWARE-ANGRIFFE)

**7 von 10
Industriebetriebe
bereits betroffen**

RANSOMWARE-ANGRIFFE: ANSTIEG SEIT 2016

Nutzer sollten weiterhin aufmerksam bei unbekannten und zweifelhaften Mails sein.



SPAM-MAILS MIT SCHAD.SOFTWARE



SPAM-MAILS MIT SCHADPROGRAMM-ANHÄNGEN LEGEN WEITER ZU

Im ersten Halbjahr 2016 nahm die gesamte Spamaktivität im Vergleich zum Vorjahr um **73%** zu. Im Bereich des klassischen Spams aber nur eine Zunahme von **16%**.

Schadsoftware, die per Spam-Mails verbreitet wird, hat hingegen um **1.270%** extrem zugelegt.

Immer mehr Varianten verbreiten sich in kurzer Zeit und setzen so die klassischen Abwehrmaßnahmen außer Kraft: 2016 wurden täglich rund

380.000

neue Schadprogrammvarianten entdeckt.

OPFER VON CYBERCRIME

OPFER VON CYBER-KRIMINALITÄT ZEIGEN STRAFTATEN EHER BEI DER POLIZEI AN¹⁾



IN VERDÄCHTIGEN SITUATIONEN



IN VERDÄCHTIGEN SITUATIONEN REAGIEREN INTERNETNUTZER, INDEM SIE...²⁾

- ... die betreffende Internetseite verlassen oder E-Mail löschen **(83,4%)**
- ... sich an den Seitenbetreiber wenden **(12,9%)**
- ... sich an die Internetbeschwerdestelle wenden **(8,5%)**
- ... sich an die Polizei wenden **(26,9%)**

Nur **3,1%** der Internetnutzer reagieren in verdächtigen Situationen gar nicht.

3

0011

WIE SCHÜTZE ICH
MEIN UNTERNEHMEN?

UNTERNEHMENSSCHUTZ

1. Technischer Schutz

A. Firewalls, Virenschutz, Data Loss Prevention, IDS, IPS, etc.

B. Aufwand, Zeit und viel Geld

2. Organisatorischer Schutz

C. Richtlinien und Standards (ISO 27000, ITIL)

D. Viel Aufwand, viel Zeit und viel Dokumentation (Geld)

4

0100

5 ALLTAGSGESCHICHTEN

5 ALLTAGSGESCHICHTEN

1. Lassen Sie sich nichts Schenken
2. Überwachung des Vorstandes
3. Diebstahl von Emissionszertifikaten
4. Verdacht auf E-Bombing amerikanischer Banken
5. Elektronischer Köder hat zugeschnappt
6. KMU: Anschaffung von Zusatz-Schutz-Software um 1/4 Mio. € 2016?

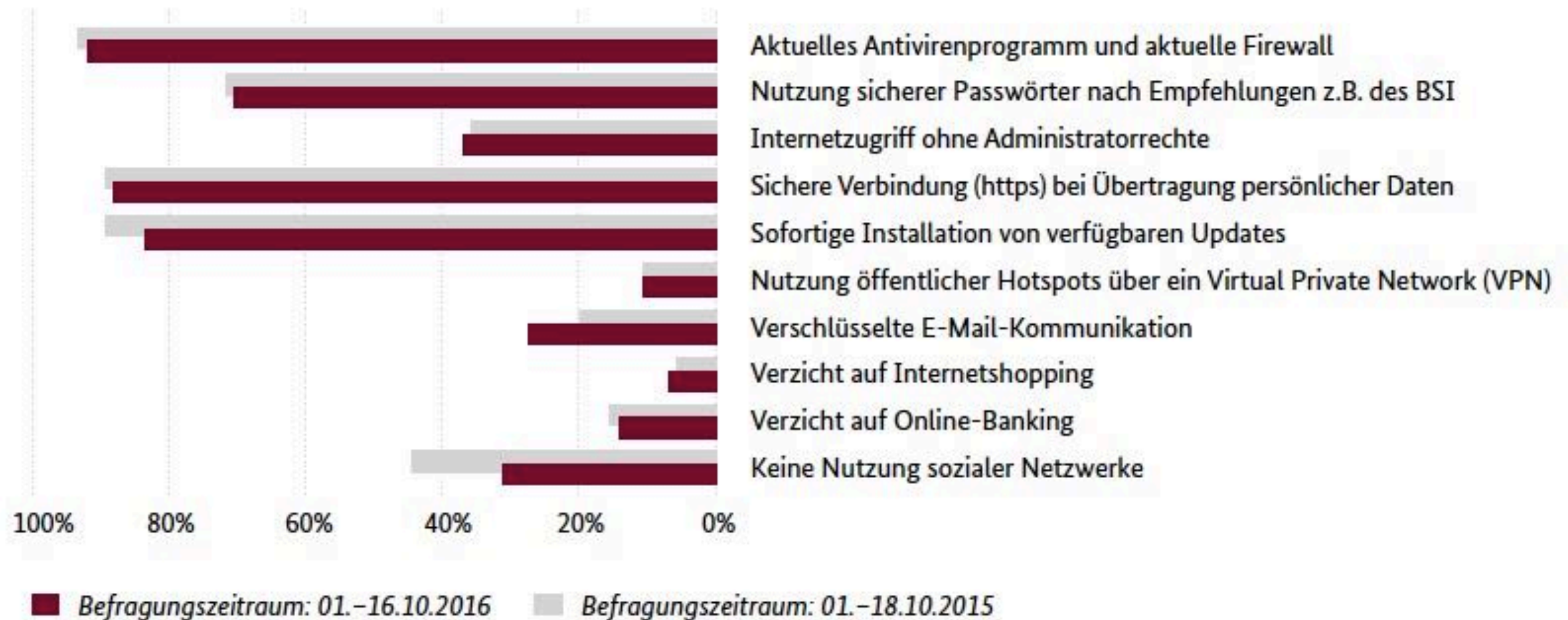
5

0100

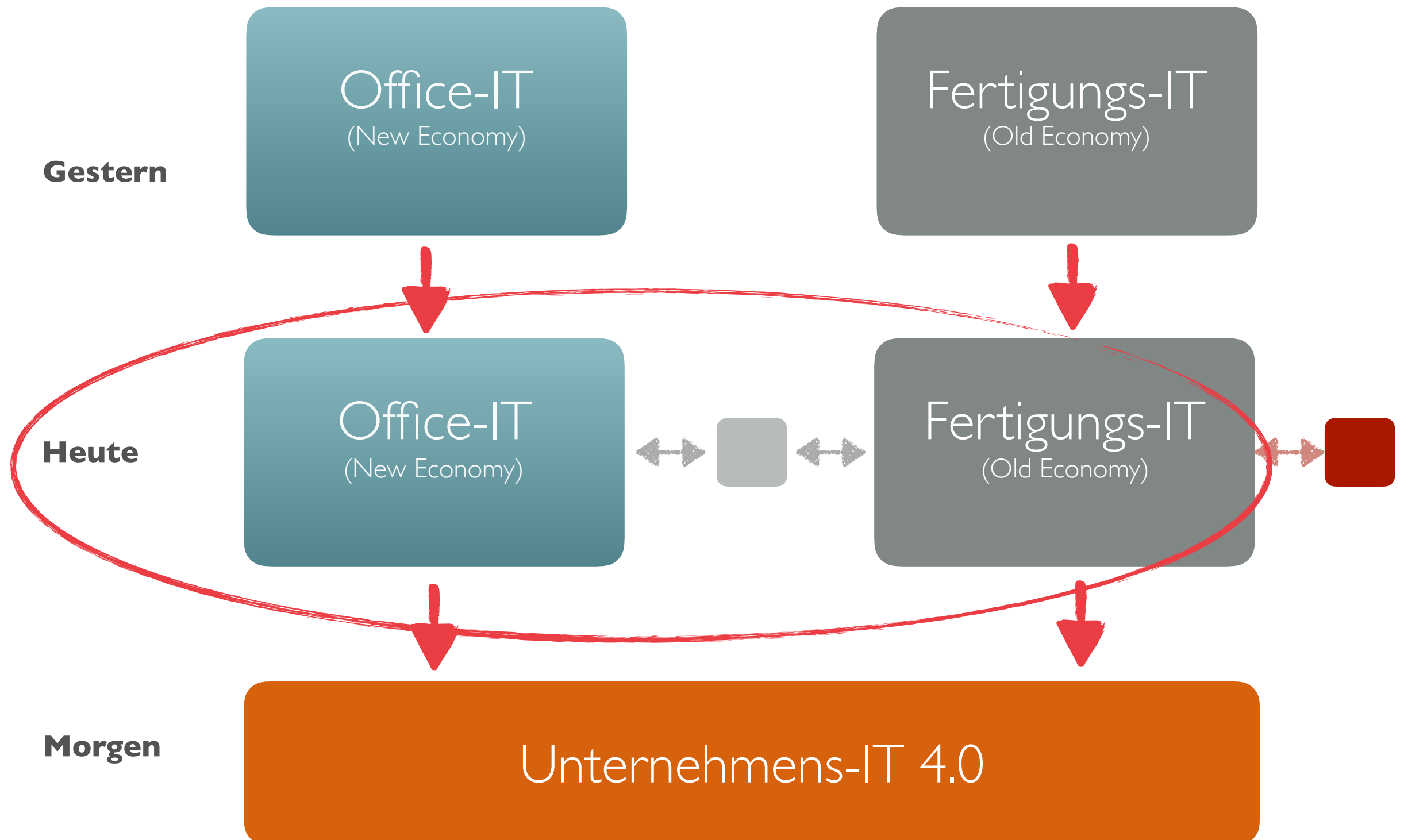
ZUSAMMENFASSUNG

MÖGLICHST WENIG AUFWAND?

MÖGLICHST WENIG AUFWAND: NUTZER GREIFEN AUF GÄNGIGE SCHUTZMASSNAHMEN ZURÜCK¹⁾



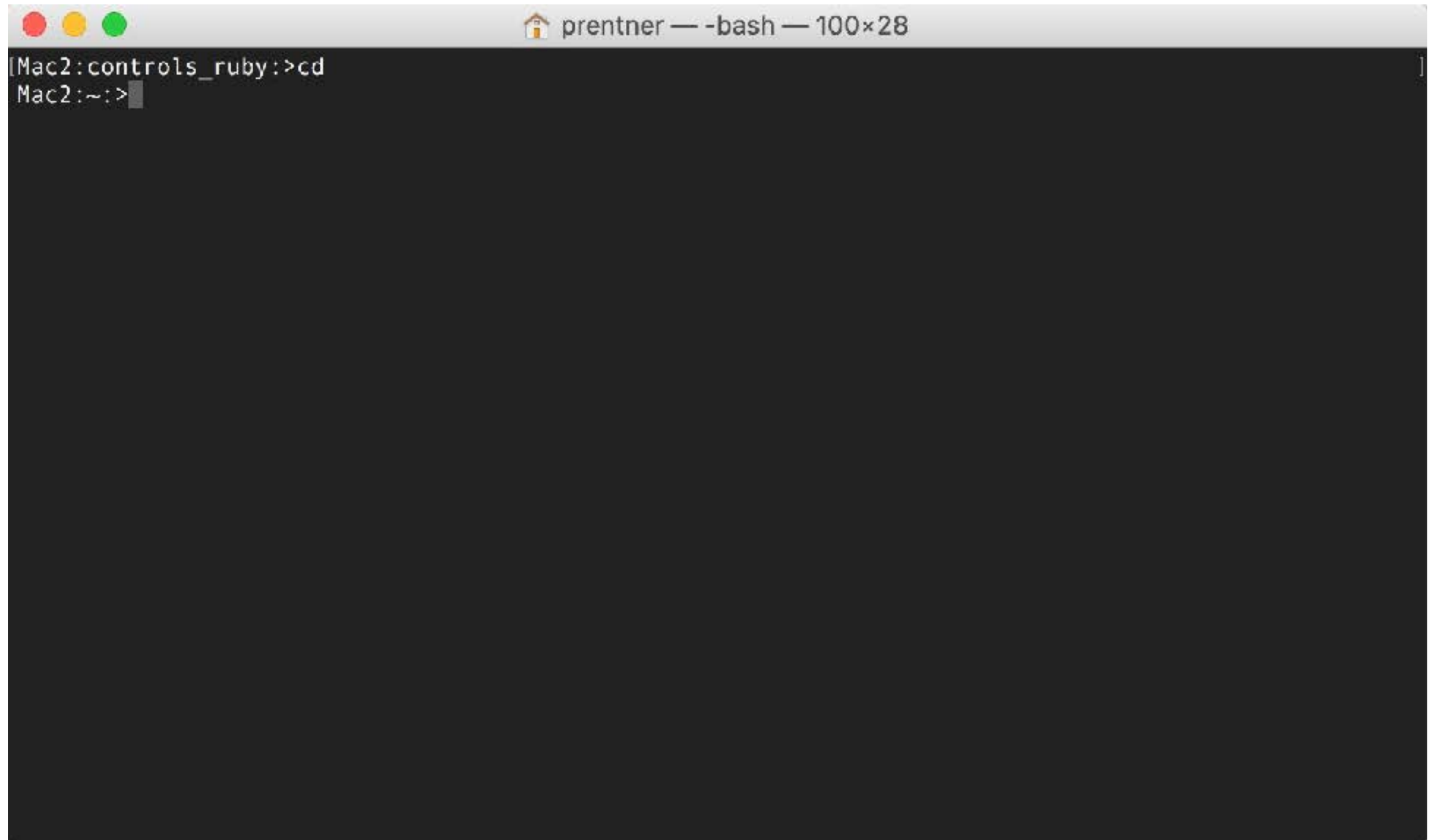
GESTERN.HEUTE.MORGEN



ZUSAMMENFASSUNG

1. Planen sie Ihre IT-Strategie für 2022
2. Sensibilisierung und Mitarbeiter-Schulungen
3. Halten Sie Ihre Unternehmenskultur hoch (Verärgern Sie keine IT-Administratoren)
4. Halten Sie Ihre Computer so sauber wie Ihr Zuhause (kümmern Sie sich jeden Tag darum)
5. Firewalls, Virenschutz, Data Loss Prevention, Intrusion Detection and Defense
6. Bauen Sie ein Informations.Sicherheits.Management.System (ISMS) auf
7. Lassen Sie Ihre IT-Systeme regelmäßig prüfen, überwachen und zertifizieren (Auslagerung der Haftung)
8. Viel Geld, klare IT-Strategien und Risikobereitschaft sind die Schlüsselfaktoren für Industrie 4.0 bis 2022.

The future of hack's is still black.

A screenshot of a macOS terminal window. The title bar at the top shows three colored window control buttons (red, yellow, green) on the left, a home icon followed by the text 'prentner — -bash — 100x28' in the center, and a close button on the right. The terminal area has a black background with white text. The first line shows a prompt '[Mac2:controls_ruby:>' followed by the command 'cd'. The second line shows a new prompt 'Mac2:~:>' with a cursor. The rest of the terminal is empty.

```
[Mac2:controls_ruby:>cd  
Mac2:~:>
```

Besten Dank für
Ihre Aufmerksamkeit!

Haben Sie noch Fragen?

