Insider-Bedrohungen

Von Unwissenheit bis zur Absicht und wie man sich am besten schützt!

Lars Eilebrecht

Die Architekten
für Informations- und Kommunikationstechnologien

DOK
ICT BUSINESS & TECHNOLOGY CONSULTING
SYSTEME

Definition

Insider-Bedrohung:

Ein **Insider** oder eine Gruppe von Insidern, der/die entweder beabsichtigt der Organisation Schaden oder Verluste zuzufügen oder bei denen es wahrscheinlich ist, das Ihr **Verhalten** dazu führt.

Insider:

Jede Person, die autorisierten Zugang zu den Ressourcen der Organisation, einschließlich Mitarbeitenden, Verfahren, Informationen, Technologie und Einrichtungen, **hat oder früher hatte**.

Insider-Bedrohungen

Unbeabsichtigt

Unwissenheit

Fehlende Prozesse

Unzulängliche Technologie

Ambivalent

Mehrere Rollen

Geteilte Verantwortlichkeiten

Fehlende Funktionstrennung

Absichtlich

(gefühlte) Benachteiligung oder ungerechte Behandlung

Finanziell motiviert

Quelle: *Schoenherr, et al., „Multiple Approach Paths to Insider Threat“, CITRAP, 2022*

In **76%**

der Informationssicherheitsvorfällen
spielt der Faktor *„Mensch“* eine Rolle.

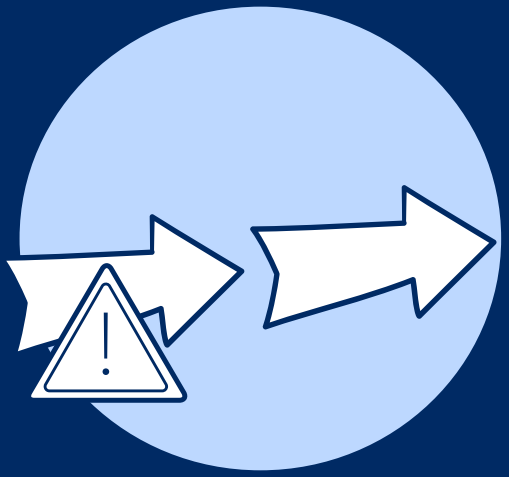
Quelle: *2024 Data Breach Investigations Report*, Verizon

DOK
ICT BUSINESS & TECHNOLOGY CONSULTING
SYSTEME

Kategorien der Primäre Bedrohungen und Risiken

Menschen

Technologie

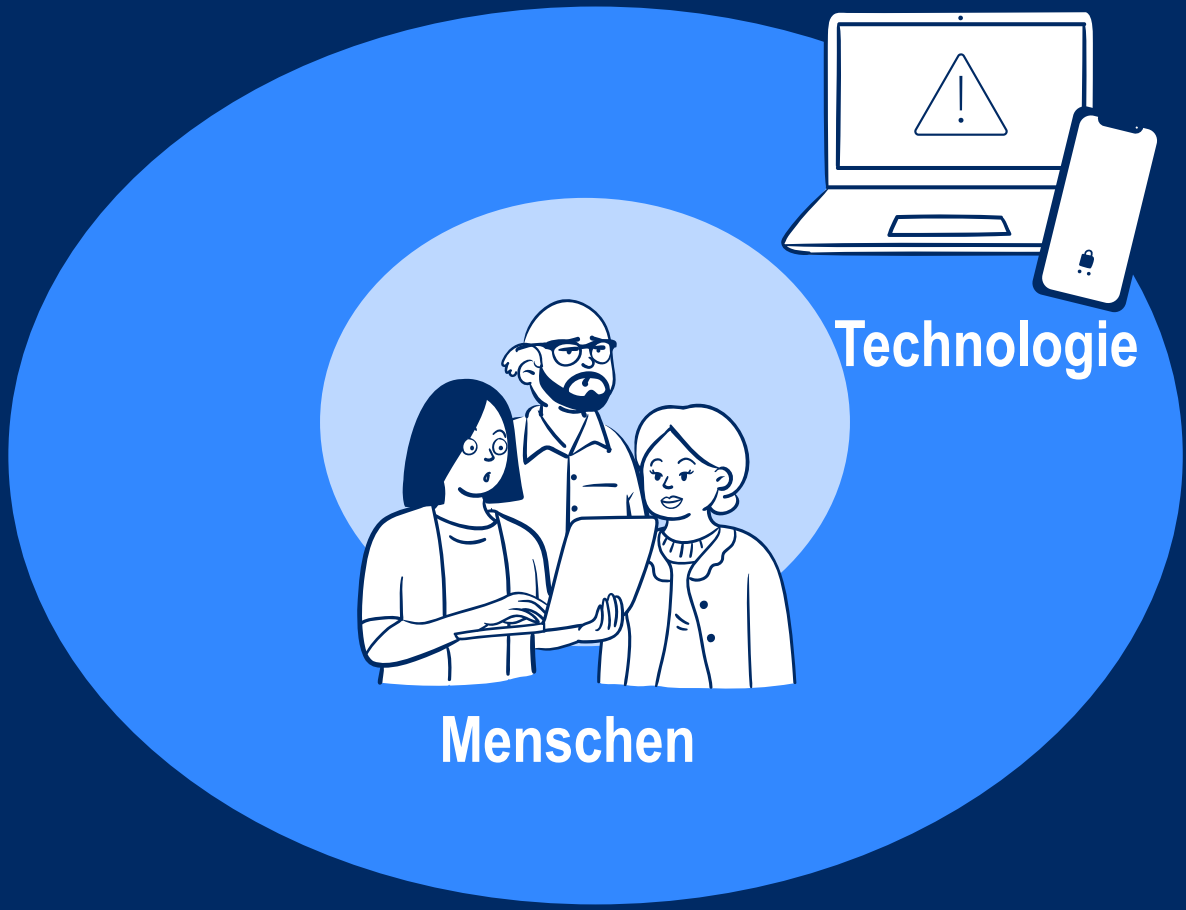


Prozesse

Primäre Bedrohungen und Risiken

Menschen

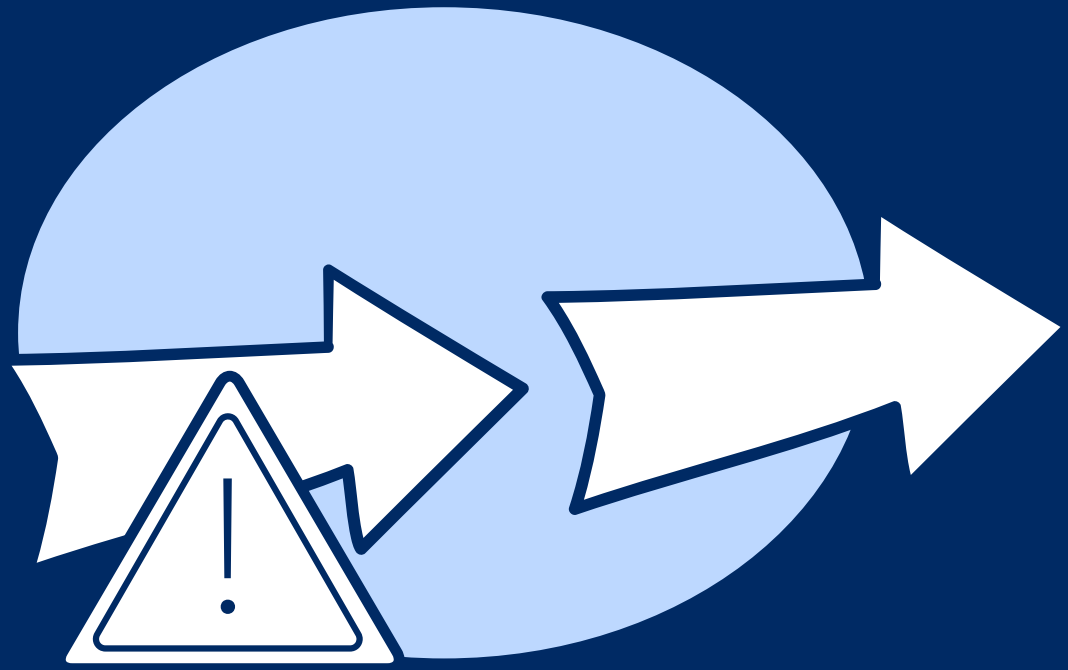
Primäre Bedrohungen und Risiken



Primäre Bedrohungen und Risiken

Primäre Bedrohungen und Risiken

Prozesse



Problem:

Ungenügende Erkennung von Bedrohungen

© kyle-glenn-unsplash

Erkennen von Bedrohungen

Kontinuierliche Überwachung

Verhaltensanalyse

Regelmäßige Auditierung

Notfallplan erstellen

Problem:

Unzureichende Zugriffskontrolle

© bryan-natanael-unsplash

Zugriffskontrolle

Principle of Least Privilege

Rollenbasierte Zugriffskontrolle

Regelmäßige Überprüfung

Automatisierung von Prozessen

MFA überall einsetzen

© bryan-natanael-unsplash


Problem:
Unsichere Ressourcen- und Kontoverwaltung
© bryan-natanael-unsplash

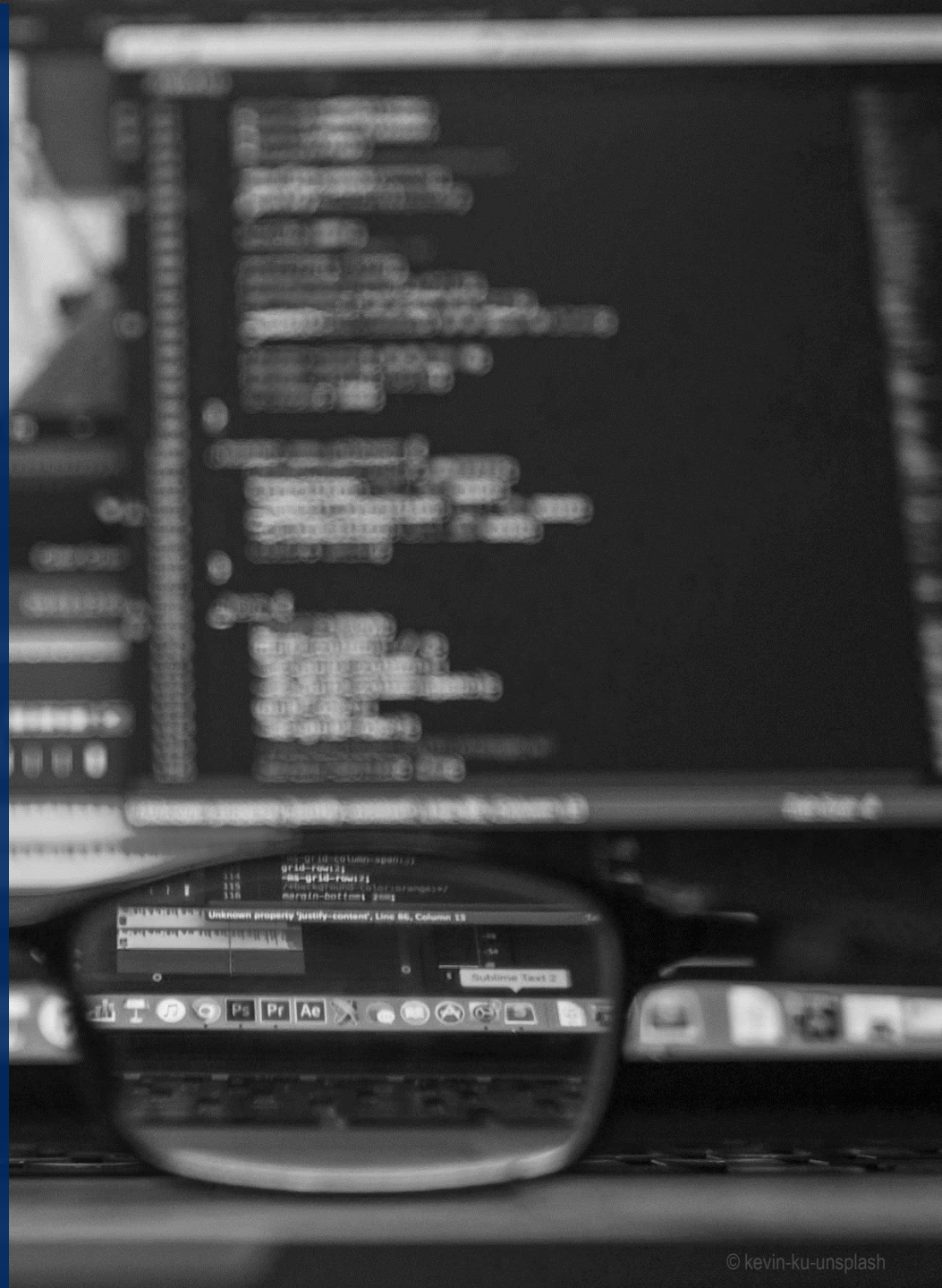
Ressourcen- und Kontoverwaltung

Protokollierung von Änderungen

Regelmäßige Überprüfung

Funktionstrennung

Sicherheitsrichtlinien und Arbeitsanweisungen




Problem:
Unzureichende Verwaltung von Vermögenswerten
© gettyImages

Verwaltung von Vermögenswerten

Inventarisierung

Lebenszyklus verfolgen

Regelmäßige Auditierung

Dokumentations-Standards

© gettyImages

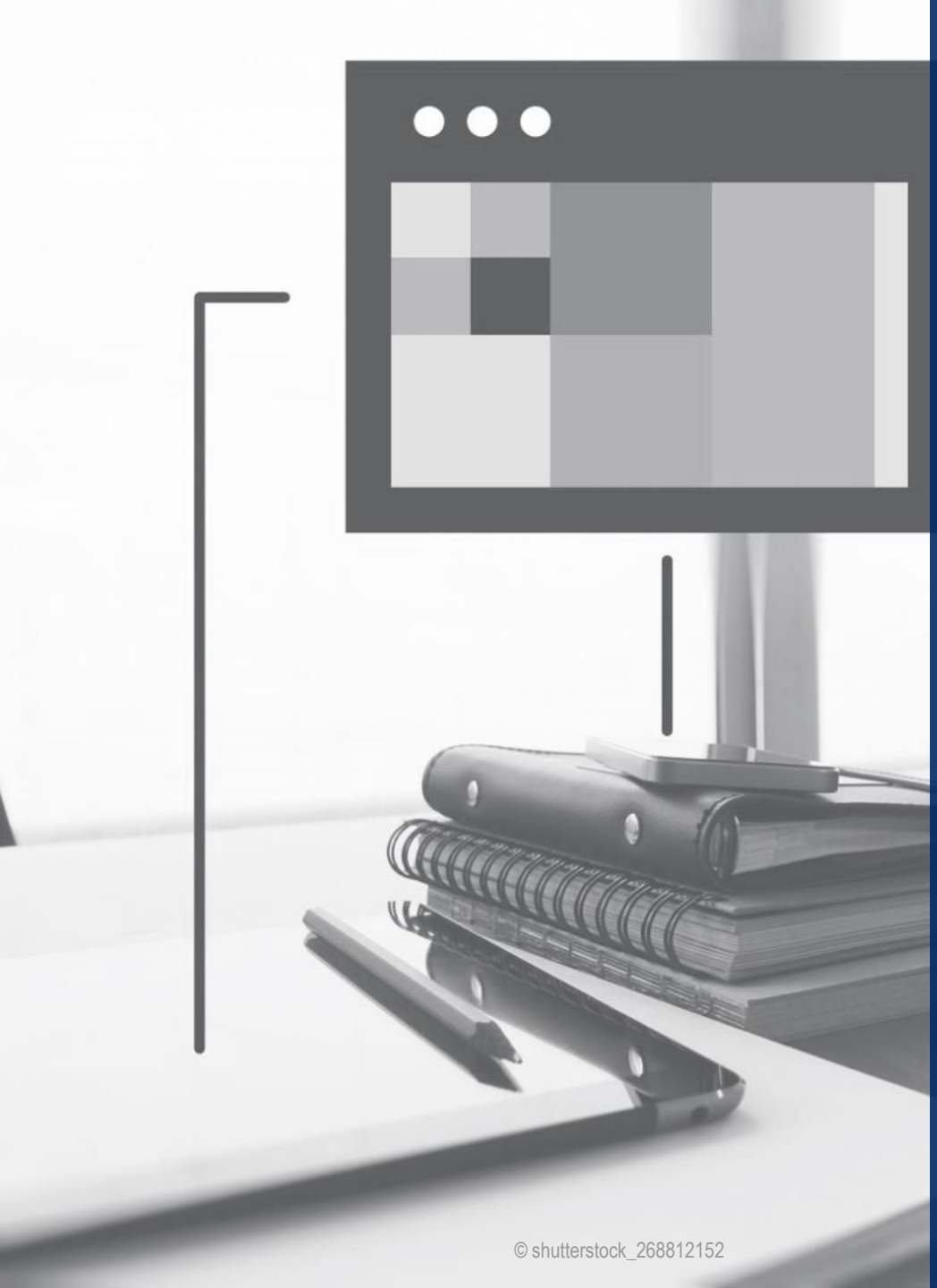
Primäre Bedrohungen und Risiken

Technologie

Problem:

Veraltete und ungepatchte Software

© shutterstock_268812152



Ungepatchte Software

Regelmäßige, zeitnahe Updates

Schwachstellen-Scanning

Patch-Management-Prozesse

Ersetzen von Altsystemen

Hersteller-Support

Problem:

Unsichere Konfiguration und Netzwerkverwaltung

© shutterstock_656932525


© shutterstock_656932525

Konfiguration und Netzwerkverwaltung

Konfigurationsmanagement

Konfigurations-Baseline

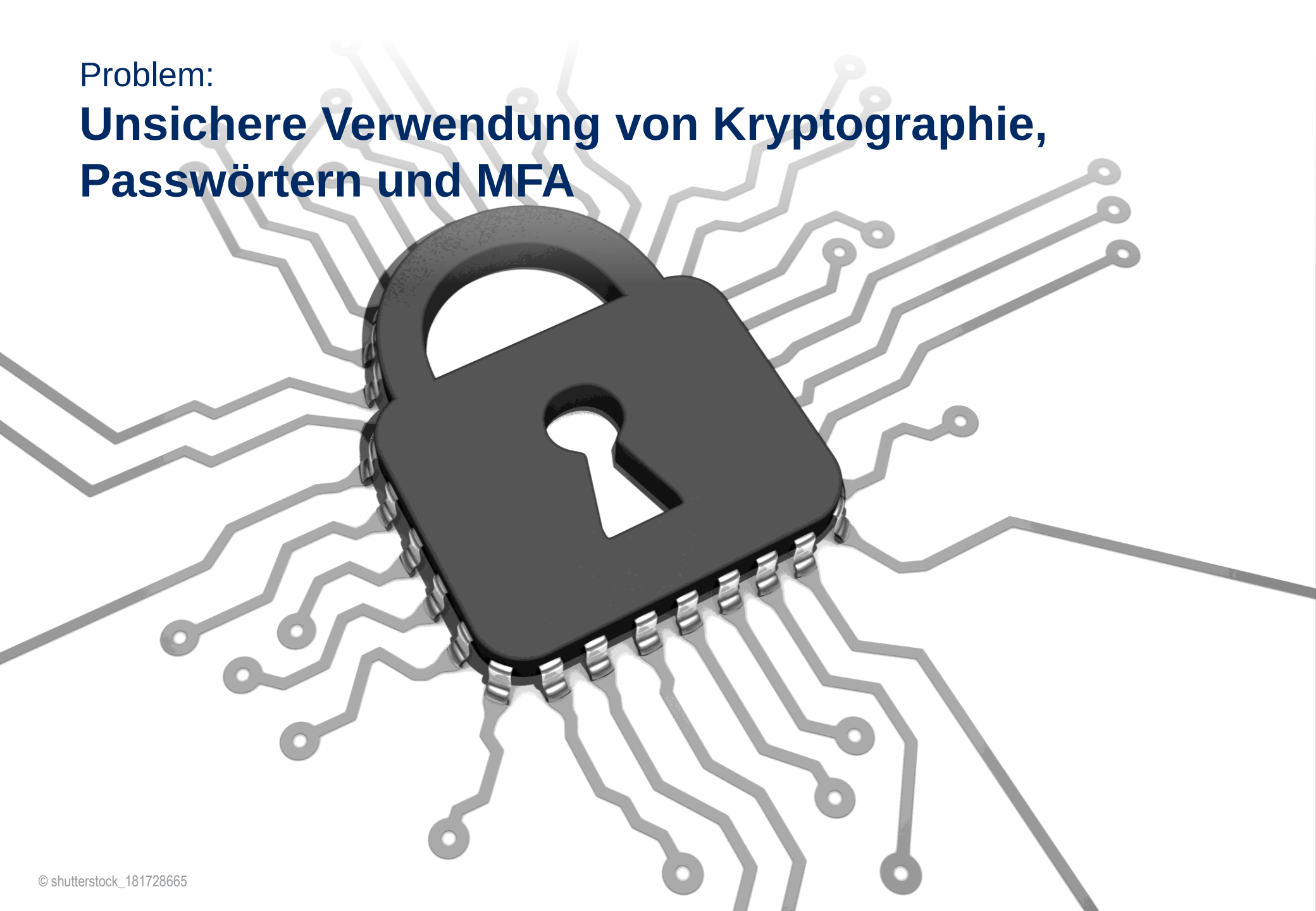
Zero Trust und Segmentierung

Zugangs- und Zugriffskontrolle

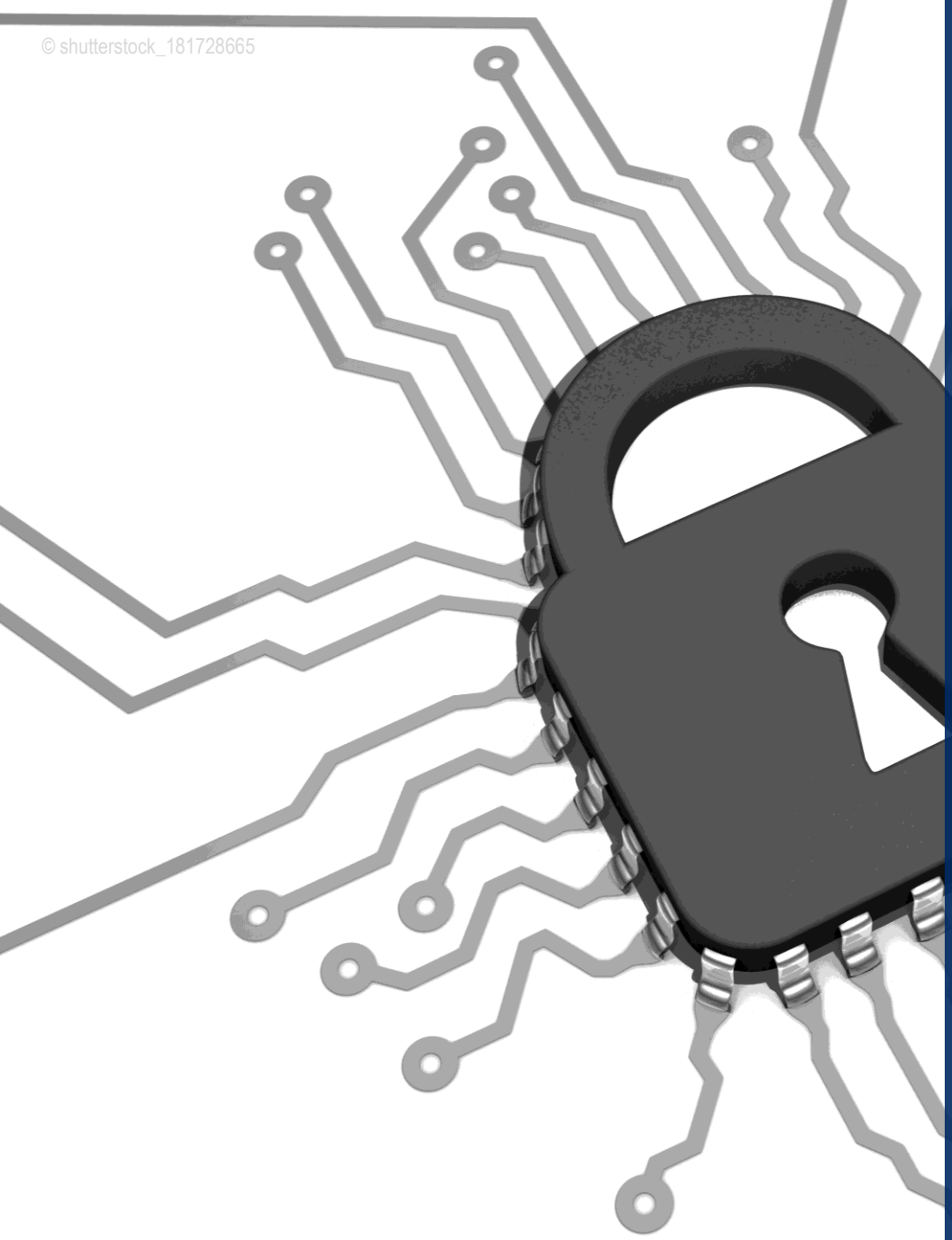
Kontinuierliche Überwachung & Automatisierung

Problem:

Unsichere Verwendung von Kryptographie, Passwörtern und MFA



© shutterstock_181728665


© shutterstock_181728665

Kryptographie, Passwörter und MFA

- Starke krypt. Algorithmen
- Schlüsselverwaltung
- Sicherheitsrichtlinien
- Hersteller-Logins ändern
- Sichere Verwendung von MFA

Primäre Bedrohungen und Risiken

Menschen

© shutterstock_373567063


© shutterstock_373567063

Befähigung von Personen

Schulungen

Sicherheitsbewusstsein

Mechanismen zur Meldung

Problem:

Verärgerte Mitarbeitende

© vitaly-gariev-unsplash

Verhalten und Stimmung

Stimmungsbeobachtung

Effektive Beschwerdewege

Proaktives Management

Unterstützungssysteme

Problem:

Beteiligung externe Dienstleister

© shutterstock_587502440

© shutterstock_587502440

Externe Dienstleister sicher einbinden

- Strenge Sicherheitsrichtlinien & Arbeitsanweisungen
- Regelmäßige Auditierung
- Limitierte Zugriffsrechte
- Vertragliche Verpflichtungen
- Informationssicherheitsschulung

Zusammenfassung

- ✓ Ganzheitliche Betrachtung
- ✓ Fortlaufender Prozess
- ✓ Sicherheitsbewusste Kultur
- ✓ Sicherheitsstrategie

Informationssicherheit ist nicht alleine durch technische Maßnahmen zu erreichen.

Der Mensch stellt einen zentralen und wichtigen Teil der Sicherheitsstrategie des Unternehmens dar.

Mit durchdachten Strukturen, Prozessen, passender Technologie und einer sicherheitsbewussten Unternehmenskultur kann man Insider-Bedrohungen effizient entgegenwirken.

Die Architekten

für Informations- und Kommunikationstechnologien

DOK SYSTEME
ICT BUSINESS & TECHNOLOGY CONSULTING