Securitas




# Informationssicherheit beginnt nicht am Bildschirm

Wie Unternehmen Daten, Zugänge und Informationen ganzheitlich schützen




Inhalt

Informationssicherheit endet nicht bei der IT 2
Die Angriffsfläche hat sich verändert 4
Wenn der Anlass Teil des Angriffs wird 6
Informationssicherheit beginnt im Alltag 8
Der Lebenszyklus einer Information 10
Der physische Schutz von Informationen 12
Der Mensch bleibt Teil des Sicherheitskonzepts 14
Vom Erkennen zum Reagieren 16
10 Maßnahmen für ganzheitliche Informationssicherheit 18

# Informationssicherheit endet nicht bei der IT

**Das Wichtigste auf einen Blick**

Informationssicherheit umfasst digitale, physische und organisatorische Risiken.

Entscheidend ist nicht nur, wo Informationen gespeichert sind, sondern wer wann und wie auf sie zugreifen kann.

Ein ganzheitlicher Ansatz verbindet Menschen, Prozesse, Technologie und physische Schutzmaßnahmen.

Der Schutz muss den Informationen durch das Unternehmen folgen, nicht nur den IT-Systemen.

Ein vertrauliches Dokument bleibt nach einem Meeting im Raum liegen. Ein geschäftlich genutztes Smartphone geht auf einer Reise verloren. Mitarbeitende erhalten eine täuschend echte Nachricht mit der Aufforderung, ihre Zugangsdaten zu bestätigen. Ein Datenträger wird ausgemustert, ohne dass klar geregelt ist, wie die darauf gespeicherten Informationen sicher gelöscht werden.

Die Situationen unterscheiden sich. Das Risiko dahinter ist dasselbe: Schützenswerte Informationen können offengelegt, manipuliert, verloren oder für Unbefugte zugänglich werden.

Informationssicherheit wird dennoch häufig zuerst mit IT-Sicherheit verbunden. Firewalls, sichere Passwörter, Multi-Faktor-Authentifizierung und Schutz vor Cyberangriffen sind wichtige Bausteine. Sie decken jedoch nur einen Teil der möglichen Risiken ab.

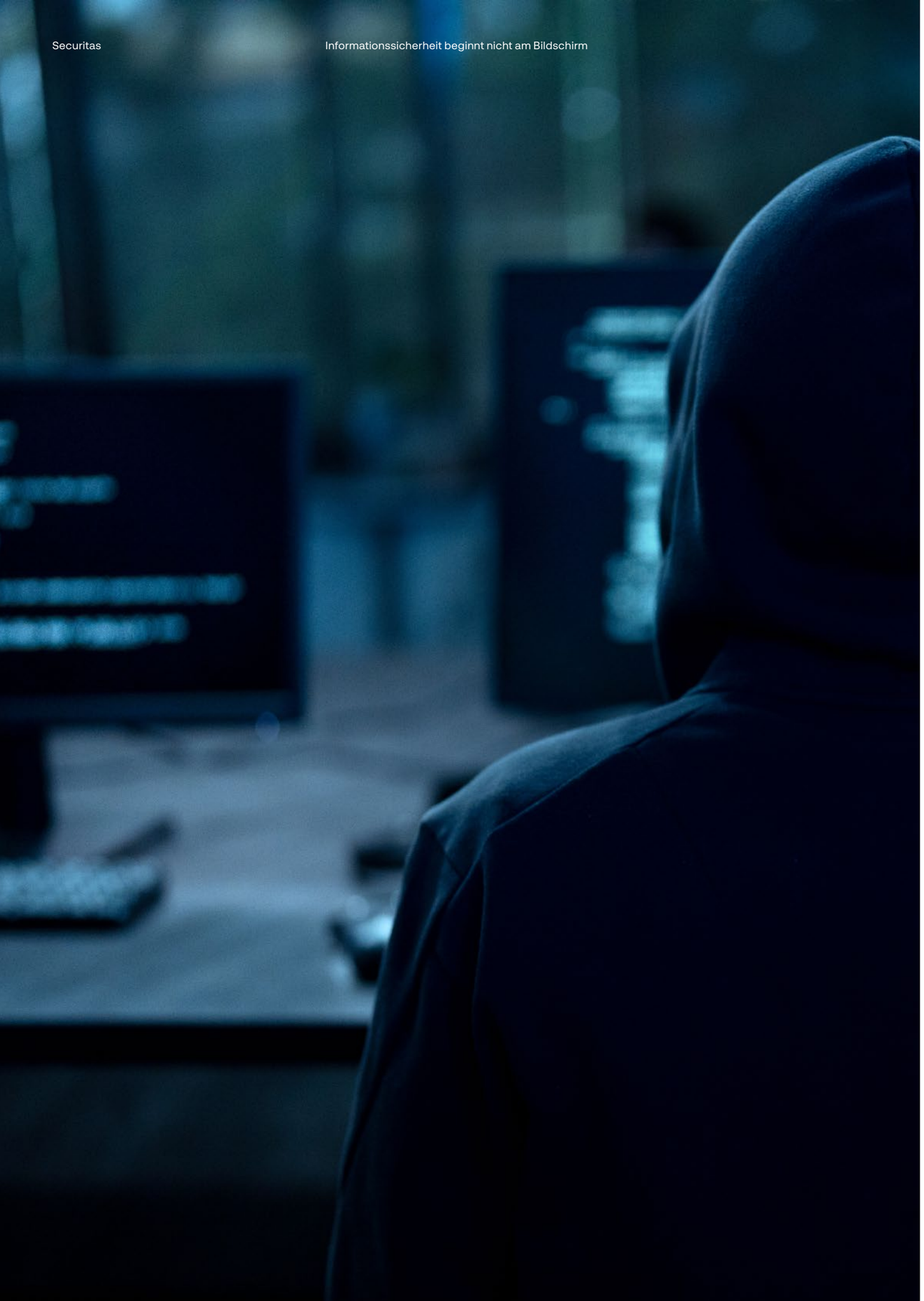
Informationen wechseln im Unternehmensalltag permanent zwischen digitaler und physischer Welt. Sie werden erstellt, gespeichert, geteilt, ausgedruckt, archiviert, auf mobilen Geräten mitgeführt und schließlich gelöscht oder vernichtet. Gleichzeitig greifen Menschen an unterschiedlichen Standorten und mit unterschiedlichen Berechtigungen darauf zu.

Deshalb muss der Schutz von Informationen ihrem tatsächlichen Weg durch das Unternehmen folgen.

Ganzheitliche Informationssicherheit verbindet Menschen, Prozesse, Technologie und physische Schutzmaßnahmen.

Gerade für Unternehmen mit komplexen Standorten, sensiblen Betriebsprozessen oder erhöhten regulatorischen Anforderungen gewinnt diese integrierte Betrachtung an Bedeutung. Genau diese Faktoren charakterisieren auch die im Securitas ICP beschriebenen Unternehmen mit erhöhtem Sicherheitsbedarf.





# Die Angriffsfläche hat sich verändert

Cyberangriffe richten sich nicht ausschließlich gegen technische Schwachstellen. Häufig versuchen Angreifer ganz gezielt, menschliches Verhalten auszunutzen.

Dazu gehören vermeintlich vertraute Situationen, Autorität, Zeitdruck oder die Aufforderung, eine alltägliche Handlung auszuführen. Die Methoden entwickeln sich dabei kontinuierlich weiter.

### PHISHING UND SPEAR-PHISHING

Phishing-Nachrichten sollen Empfänger beispielsweise dazu bewegen, Links zu öffnen, Anhänge herunterzuladen oder Zugangsdaten einzugeben.

Spear-Phishing geht einen Schritt weiter. Die Kommunikation wird gezielt auf eine Person, deren Funktion oder ein konkretes geschäftliches Umfeld zugeschnitten. Je plausibler Absender, Kontext und Anliegen erscheinen, desto schwieriger wird es, einen Angriff unmittelbar zu erkennen.

### SMISHING UND VISHING

Auch Smartphones und Telefonie sind Teil der Angriffsfläche.

Beim Smishing werden betrügerische SMS oder Messenger-Nachrichten eingesetzt. Beim Vishing (Voice-Phishing) versuchen Angreifer telefonisch, an Informationen zu gelangen oder bestimmte Handlungen auszulösen.

Ein vermeintlicher Anruf vom IT-Support kann dabei ebenso Teil eines Angriffs sein wie eine SMS eines angeblichen Paketdienstes.

### QUISHING

Beim Quishing verbirgt sich der Link hinter einem QR-Code. Das erschwert die unmittelbare Einschätzung des tatsächlichen Ziels.

Insbesondere QR-Codes in E-Mails, auf Aushängen oder im öffentlichen Raum sollten deshalb nicht grundsätzlich als vertrauenswürdig betrachtet werden. Vor dem Öffnen sollte geprüft werden, wohin der hinterlegte Link tatsächlich führt.

### DAS VERBINDENDE ELEMENT: SOCIAL ENGINEERING

Die Angriffskanäle unterscheiden sich. Das Prinzip dahinter bleibt häufig gleich.

Angreifer versuchen, eine Situation zu erzeugen, in der Menschen handeln, bevor sie die Legitimität einer Anfrage ausreichend geprüft haben.

Weitere Formen von Social Engineering sind beispielsweise:

- CEO Fraud: Angreifer geben sich als Führungskraft aus und fordern etwa dringende Überweisungen oder die Weitergabe vertraulicher Informationen.
- Fake IT Support: Ein vermeintlicher IT-Mitarbeiter fordert Zugangsdaten, Sicherheitscodes oder den Zugriff auf ein Gerät.
- Pretexting: Unter einem glaubwürdigen Vorwand wird versucht, vertrauliche Informationen zu erhalten oder bestimmte Handlungen auszulösen.
- Business Email Compromise (BEC): Geschäftliche Kommunikationsabläufe werden imitiert oder manipuliert, um beispielsweise Zahlungen oder sensible Informationen umzuleiten.
- Tailgating: Unbefugte verschaffen sich Zugang zu geschützten Bereichen, indem sie berechtigten Personen unbemerkt oder unter einem Vorwand folgen.

Eine wirksame Informations-sicherheitsstrategie muss daher technische Schutzmaßnahmen mit Awareness und klaren Prozessen für verdächtige Situationen verbinden.

# Wenn der Anlass Teil des Angriffs wird

Bestimmte Ereignisse und Jahreszeiten bieten Cyberkriminellen einen besonders glaubwürdigen Kontext.

Rund um Black Friday und Weihnachten steigt beispielsweise die Zahl legitimer Bestellbestätigungen, Paketankündigungen, Rabattaktionen und Zahlungsinformationen. Gefälschte Nachrichten können dadurch im normalen Kommunikationsaufkommen weniger auffallen.

Auch andere Anlässe lassen sich instrumentalisieren. Rund um den Valentinstag können vermeintliche Gutscheine, persönliche Nachrichten oder Gewinnspiele als Köder dienen. In Ferienzeiten können Abwesenheiten und Vertretungssituationen ausgenutzt werden.

Der Computer Security Day am 30. November bietet deshalb einen passenden Zeitpunkt, um gerade auf diese saisonalen Risiken aufmerksam zu machen: Er fällt unmittelbar in eine Phase, in der Black Friday, Cyber-Angebote, Weihnachtsgeschäft und erhöhtes Paketaufkommen zahlreiche plausible Anlässe für Phishing, Smishing und Quishing liefern.

Für Unternehmen ist dabei weniger der einzelne Anlass entscheidend als das zugrunde liegende Muster:

- Ist die Kontaktaufnahme unerwartet?
- Wird ungewöhnlicher Zeitdruck aufgebaut?
- Sollen Zugangsdaten oder Sicherheitscodes mitgeteilt werden?
- Führt ein Link oder QR-Code zu einem unbekannten Ziel?
- Weicht eine Anfrage von üblichen Prozessen ab?
- Fordert eine vermeintlich bekannte Person eine ungewöhnliche Handlung?

Je plausibler der Anlass erscheint, desto wichtiger ist eine unabhängige Prüfung der Anfrage.



# Informationssicherheit beginnt im Alltag

Nicht jeder Sicherheitsvorfall ist das Ergebnis eines gezielten Angriffs.

Viele Risiken entstehen im normalen Arbeitsalltag: durch veraltete Software, unnötige Zugriffsrechte, ungesperrte Geräte, nicht mehr benötigte Benutzerkonten oder sensible Dokumente, die offen zugänglich bleiben. Digitale Hygiene sollte deshalb als Teil des laufenden Informationssicherheitsmanagements verstanden werden.

Dazu gehören insbesondere:

- **Systeme aktuell halten.**
  Betriebssysteme, Software und Apps sollten regelmäßig aktualisiert und bekannte Sicherheitslücken zeitnah geschlossen werden.

- **Nicht mehr benötigte Anwendungen und Accounts entfernen.**
  Jeder zusätzliche Account und jede Anwendung erweitert potenziell die Angriffsfläche.

- **Zugriffsrechte regelmäßig überprüfen.**
  Berechtigungen sollten sich am tatsächlichen Bedarf orientieren. Wechselt eine Person die Funktion oder endet ein Projekt, müssen auch die entsprechenden Zugriffsrechte angepasst werden.

- **Arbeitsgeräte schützen.**
  Notebooks, Smartphones und Tablets sollten gesperrt werden, sobald sie unbeaufsichtigt sind. Für mobile Geräte sind kurze automatische Sperrzeiten, aktuelle Betriebssysteme und sichere Authentifizierungsverfahren besonders relevant.

- **MFA einsetzen.**
  Multi-Faktor-Authentifizierung schafft eine zusätzliche Sicherheitsebene für Benutzerkonten und Anwendungen.

- **Passwörter sicher verwenden.**
  Für jeden Zugang sollten starke, einzigartige Passwörter oder Passphrasen verwendet werden. Zugangsdaten müssen vertraulich behandelt und dürfen **nicht** mehrfach genutzt werden. Ergänzend erhöht Multi-Faktor-Authentifizierung den Schutz, falls ein Passwort kompromittiert wird.





# Der Lebenszyklus einer Information

Informationen verändern ihren Ort, ihr Format und häufig auch ihren Schutzbedarf.

Ein Dokument wird erstellt, bearbeitet, geteilt, gespeichert, archiviert und irgendwann gelöscht. Ein digitaler Datensatz kann zum Ausdruck werden. Informationen aus einer Anwendung können auf ein mobiles Endgerät gelangen. Projektdaten können nach Abschluss des Projekts weiterhin in unterschiedlichen Systemen vorhanden sein.

Deshalb sollte Informationssicherheit den vollständigen Lebenszyklus einer Information berücksichtigen.

**ERSTELLEN UND KLASSIFIZIEREN**
Bereits bei der Erstellung sollte klar sein, welchen Schutzbedarf eine Information besitzt.

**SPEICHERN**
Der Schutzbedarf bestimmt mit, in welchen Systemen und Anwendungen Informationen gespeichert werden dürfen.

**ZUGREIFEN**
Berechtigungen sollten nach dem Need-to-know-Prinzip vergeben und regelmäßig überprüft werden. Das heißt: Mitarbeitende erhalten nur Zugriff auf die Informationen, die sie für ihre konkreten Aufgaben benötigen. Ändern sich Aufgaben oder Zuständigkeiten, müssen die Berechtigungen entsprechend angepasst und nicht mehr benötigte Zugriffsrechte entzogen werden.

**WEITERGEBEN**
Vor der Weitergabe sensibler Informationen muss geklärt sein, ob Empfänger, Kommunikationsweg und verwendetes System geeignet sind.

**ARCHIVIEREN**
Auch Informationen, die nicht mehr aktiv genutzt werden, benötigen einen ihrem Schutzbedarf entsprechenden Zugriffsschutz.

**LÖSCHEN UND VERNICHTEN**
Am Ende des Lebenszyklus muss sichergestellt werden, dass Informationen nicht unbeabsichtigt wiederhergestellt oder von Unbefugten eingesehen werden können.

Damit entsteht eine unmittelbare Verbindung zwischen digitaler und physischer Informationssicherheit.

# Der physische Schutz von Informationen

Informationen verlassen die digitale Umgebung regelmäßig.
Sie werden ausgedruckt, auf mobilen Geräten transportiert, auf Datenträgern gespeichert oder in Archiven verwahrt. Gleichzeitig befinden sich IT-Systeme, Server und Netzwerktechnik in physischen Gebäuden und Räumen.

Damit wird auch die physische Sicherheit Teil der Informationssicherheit.

**ZUTRITT ZU SENSIBLEN BEREICHEN KONTROLLIEREN**
Serverräume, Archive, Technikbereiche oder andere sensible Zonen sollten nur für berechtigte Personen zugänglich sein.

**BESUCHER UND EXTERNE DIENSTLEISTER BERÜCKSICHTIGEN**
Nicht nur Mitarbeitende bewegen sich innerhalb eines Unternehmens. Besucher, Lieferanten und externe Dienstleister müssen in physische Sicherheitskonzepte einbezogen werden.

**DOKUMENTE SICHER AUFBEWAHREN**
Vertrauliche Unterlagen sollten nicht unbeaufsichtigt auf Schreibtischen, in Besprechungsräumen oder an Druckern zurückbleiben.

**PAPIER UND DATENTRÄGER SICHER VERNICHTEN**
Der Schutzbedarf endet nicht mit der Nutzungsdauer. Papierdokumente, Festplatten und andere Speichermedien müssen so entsorgt werden, dass schützenswerte Informationen nicht rekonstruiert werden können.





# Der Mensch bleibt Teil des Sicherheitskonzepts

Technische und physische Schutzmaßnahmen reduzieren Risiken. Sie können jedoch nicht jede Situation vorwegnehmen.

Mitarbeitende entscheiden täglich darüber, wie Informationen behandelt werden: welche Informationen geteilt werden, wer Zugriff erhält, ob ein ungewöhnlicher Vorgang hinterfragt oder ein möglicherweise sicherheitsrelevanter Vorfall gemeldet wird.

Awareness und Schulungen sind deshalb ein eigenständiger Bestandteil der Informationssicherheit.

Relevant sind insbesondere regelmäßige Trainings zu:

- Social Engineering und Phishing,
- Passwort- und Zugangssicherheit,
- Informationsklassifikation,
- mobilem Arbeiten,
- Cloud- und Datennutzung,
- physischem Informationsschutz sowie
- Erkennung und Meldung von Sicherheitsvorfällen.

# Vom Erkennen zum Reagieren

Kein Sicherheitskonzept verhindert jeden Vorfall.

Deshalb muss Informationssicherheit neben Prävention zwei weitere Fähigkeiten berücksichtigen: Erkennung und Reaktion.

Verdächtige Kommunikation, verlorene Geräte, ungewöhnliche Zugriffe oder der unbeabsichtigte Versand sensibler Informationen müssen schnell erkannt und über definierte Melde- und Eskalationswege bearbeitet werden können.

Unternehmen benötigen dafür:

- klar definierte Meldewege,
- eindeutig geregelte Verantwortlichkeiten,
- dokumentierte Reaktions- und Eskalationsprozesse,
- eine schnelle fachliche Bewertung und
- eine Sicherheitskultur, die eine frühzeitige Meldung unterstützt.



# 10 Maßnahmen für ganzheitliche Informationssicherheit

01 Informationswerte und Schutzbedarf systematisch erfassen.

02 Zugriffe konsequent nach Need-to-know vergeben.

03 Multi-Faktor-Authentifizierung für relevante Systeme einsetzen.

04 Systeme, Anwendungen und mobile Geräte aktuell halten.

05 Nicht mehr benötigte Accounts und Berechtigungen konsequent entfernen.



06 Mitarbeitende regelmäßig gegen Social Engineering sensibilisieren.

07 Physische Zugänge zu sensiblen Informationen und Systemen absichern.

08 Besucher, externe Dienstleister und mobile Arbeit in das Sicherheitskonzept einbeziehen.

09 Dokumente und Datenträger über ihren gesamten Lebenszyklus schützen, einschließlich sicherer Vernichtung.

10 Melde-, Reaktions- und Eskalationsprozesse etablieren und regelmäßig überprüfen.

securitas.de