Willkommen bei der
Schulung zur Informationssicherheit und Compliance für externe Mitarbeiter

Haftungsausschluss

- Bitte lies dir alle Seiten dieses Trainings durch.

- Diese Sicherheits- und Compliance-Schulung ist für alle externen Mitarbeiter der SAP obligatorisch.

- Beachte, dass es verschiedene Arten von externen Mitarbeitern mit unterschiedlichen Zugriffsrechten innerhalb der SAP gibt. Daher ist es möglich, dass Teile dieser Schulung auf Deine Arbeitssituation nicht zutreffen. Schließe die Schulung bitte trotzdem vollständig ab. Alle Links in dieser Schulung funktionieren nur, wenn Du mit dem SAP-Netzwerk verbunden bist. Für den Abschluss dieser Schulung ist es nicht notwendig, dass Du auf die Links zugreifen kannst.

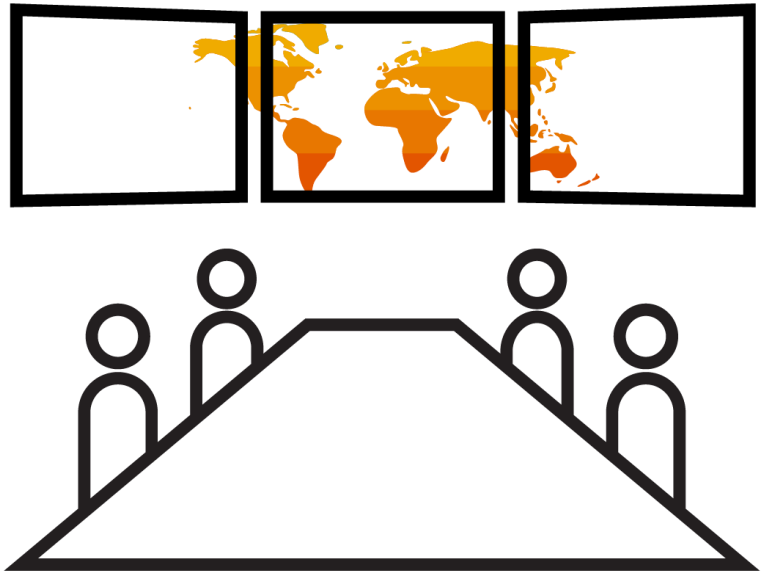
- Am Ende der Schulung musst Du Fragen in einem Test beantworten. Wenn Du den Test bestehst, erhältst Du ein Zertifikat. Dieses Zertifikat ist eine grundlegende Anforderung, um ein externer Mitarbeiter der SAP zu werden oder zu bleiben.

WARUM IST DIESE SCHULUNG ERFORDERLICH?

Große Unternehmen wie auch Privatpersonen werden zunehmend Opfer von Angriffen. Diese Vorfälle richten erheblichen Schaden an.

Außerdem schützt die Einhaltung von Compliance-Vorschriften sowohl Dich als auch die SAP.

In dieser Schulung lernst Du, Bedrohungen zu erkennen, und erfährst, was Du tun kannst, um Dich selbst und uns zu schützen.



AGENDA

CONFIDENTIAL
SOCIAL ENGINEERING
KENNWÖRTER
KLASSIFIZIERUNG VON INFORMATIONEN
SICHERER ARBEITSPLATZ
PHISHING
SOZIALE MEDIEN
SICHERE KOMMUNIKATION
Compliance-Grundlagen
Zusammenarbeit mit Dritten
TEST

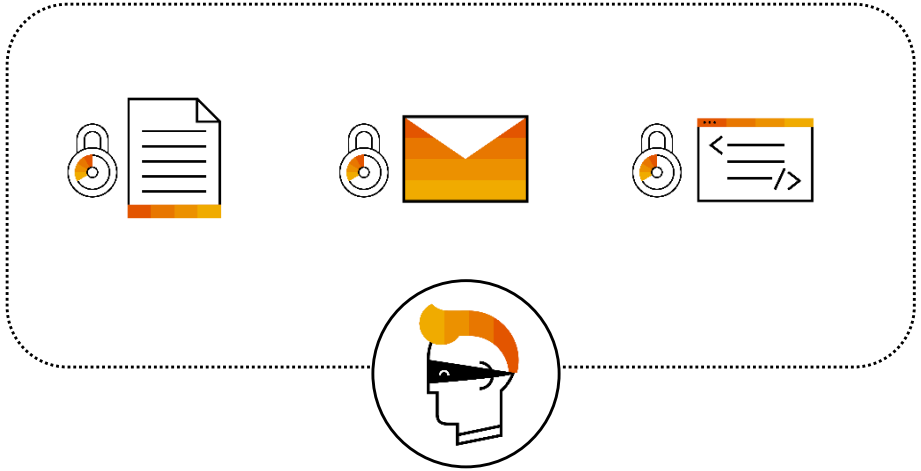
Social Engineering

Social Engineering bedeutet, dass sich jemand Informationen beschafft oder dies versucht, indem er eine Person mit Tricks verleitet oder überredet, sensible Daten preiszugeben.

In diesem Teil lernst Du, solche Tricks zu erkennen, damit Du sensible Daten nicht an Unbefugte weitergibst.

DAS RISIKO

- Die Angreifer bauen eine vertrauensvolle Beziehung auf und nutzen diese dann aus, um an vertrauliche Informationen zu gelangen.



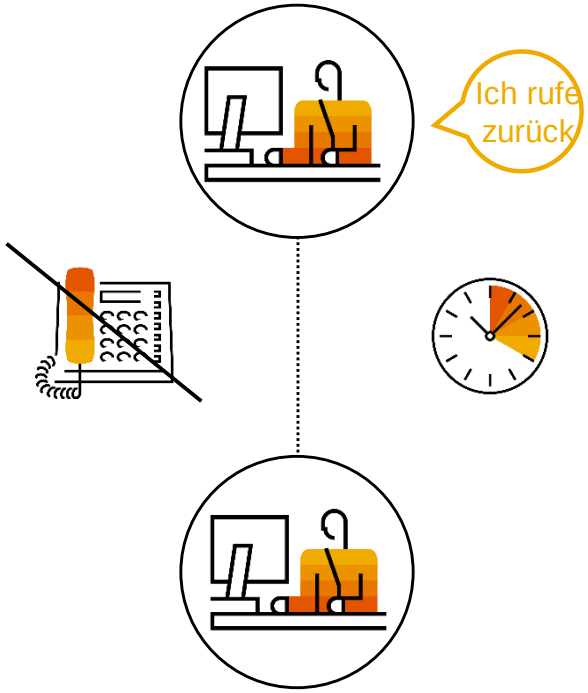
DAS RISIKO

! Die Angreifer bauen eine vertrauensvolle Beziehung auf und nutzen diese dann aus, um an vertrauliche Informationen zu gelangen.

WAS KANN ICH TUN?

1 Im Zweifel das Gespräch beenden

Wenn Du einen verdächtigen Anruf von einer unbekannten Person erhältst, beendest Du am besten das Gespräch und sagst dem Anrufer, Du hättest gerade keine Zeit und würdest zurückrufen.



DAS RISIKO

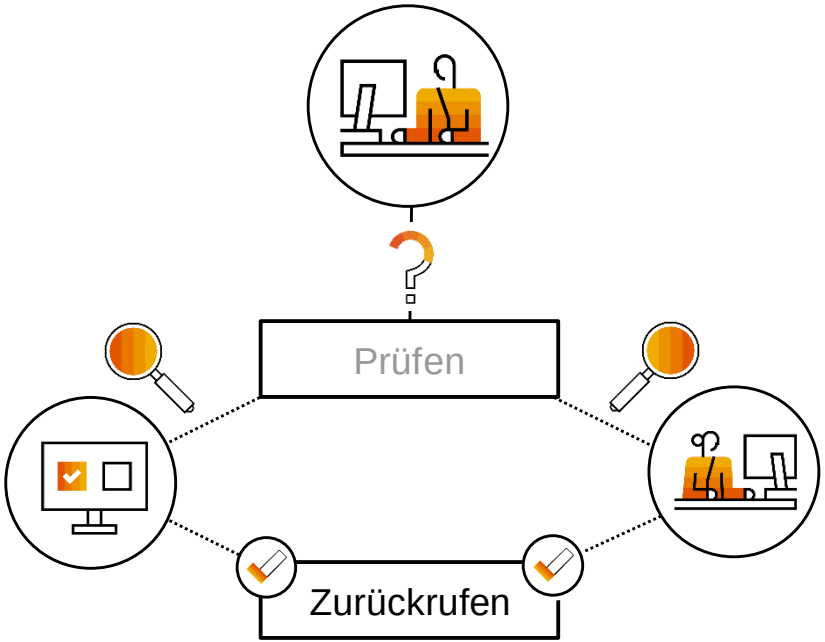
! Die Angreifer bauen eine vertrauensvolle Beziehung auf und nutzen diese dann aus, um an vertrauliche Informationen zu gelangen.

WAS KANN ICH TUN?

2 Anrufer überprüfen

Du kannst überprüfen, ob der Anrufer wirklich ist, wer er zu sein vorgibt, indem Du in der Zentrale des angeblichen Unternehmens anrufst und bittest, durchgestellt zu werden. Rufe auf keinen Fall eine Mobiltelefonnummer an, die Dir der verdächtige Anrufer möglicherweise gegeben hat.

Die Authentizität des Unternehmens und des Anrufers kannst Du auch prüfen, indem Du im Internet danach suchst.



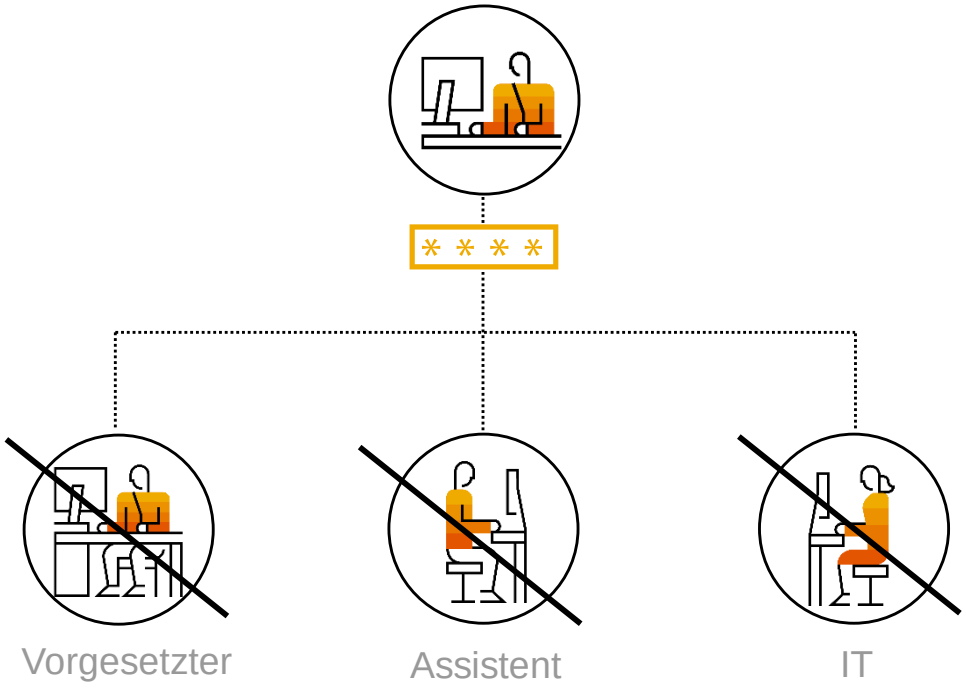
DAS RISIKO

! Die Angreifer bauen eine vertrauensvolle Beziehung auf und nutzen diese dann aus, um an vertrauliche Informationen zu gelangen.

WAS KANN ICH TUN?

3 Keine Informationen weitergeben

Gib niemals sensible Daten an unbekannte Personen weiter, weder per Telefon noch per E-Mail. Verrate niemals Dein Kennwort, nicht einmal IT-Administratoren oder Vorgesetzten.



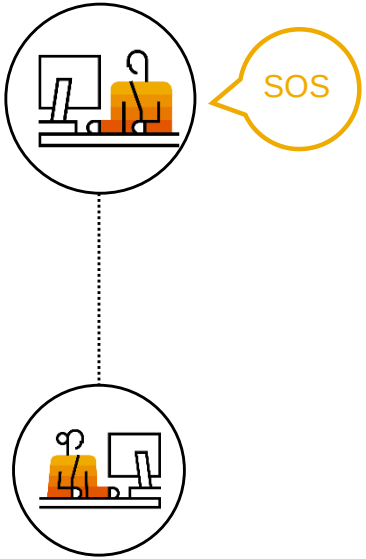
DAS RISIKO

! Die Angreifer bauen eine vertrauensvolle Beziehung auf und nutzen diese dann aus, um an vertrauliche Informationen zu gelangen.

WAS KANN ICH TUN?

4 Potenzielle Angriffe melden

Melde solche Angriffe immer sofort als Sicherheitsvorfall. Oft werden in einem Unternehmen mehrere Personen gleichzeitig ins Visier genommen. Deshalb müssen wir schnell reagieren. Bitte nutze dafür unser Incident-Reporting-Tool. Bei einem kritischen Vorfall musst Du außerdem sofort Dein lokales Sicherheitspersonal informieren.



Quick Link: go/incident-reporting

Social Engineering

Sehr gut! Du hast Folgendes gelernt:

1. Im Zweifel das Gespräch beenden
2. Anrufer überprüfen
3. Keine Informationen weitergeben
4. Potenzielle Angriffe melden

Kennwörter

Deine Kennwörter brauchst Du, um auf unsere Systeme und Daten zuzugreifen.

In diesem Teil lernst Du, gute, sichere Kennwörter für Deine Arbeit und Dein Privatleben festzulegen.

DAS RISIKO

- Unbefugte können in Deinem Namen auf Unternehmensdaten zugreifen.
- Einfache oder kurze Kennwörter lassen sich einfach erraten oder knacken.

Kennwörter schützen Deine digitale Identität. Werden sie weitergegeben, können Unbefugte auf Deine persönlichen Daten und auf Unternehmensdaten zugreifen. Einfache oder kurze Kennwörter, die nur aus wenigen Ziffern bestehen oder im Wörterbuch zu finden sind, können von Hackern einfach erraten oder geknackt werden.

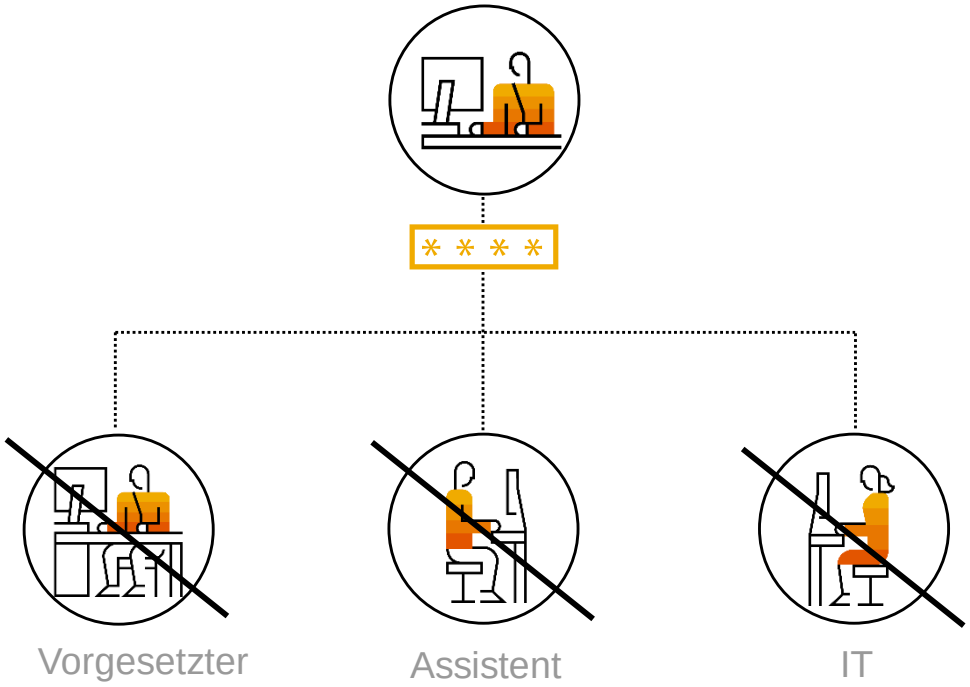
DAS RISIKO

- Unbefugte können in Deinem Namen auf Unternehmensdaten zugreifen.
- Einfache oder kurze Kennwörter lassen sich einfach erraten oder knacken.

WAS KANN ICH TUN?

1. Niemals Dein Kennwort verraten

Nicht einmal IT-Mitarbeitern oder Vorgesetzten.



DAS RISIKO

! Unbefugte können in Deinem Namen auf Unternehmensdaten zugreifen.

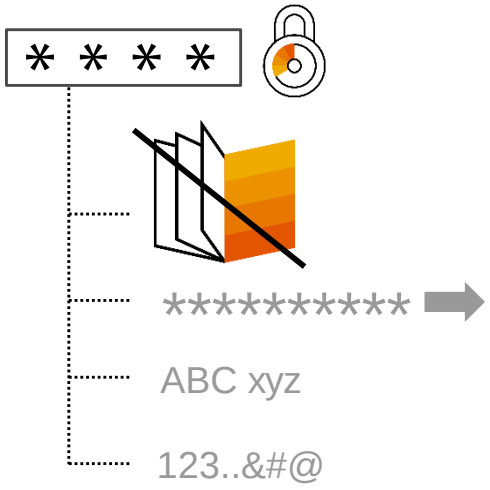
! Einfache oder kurze Kennwörter lassen sich einfach erraten oder knacken.

WAS KANN ICH TUN?

2 Immer sichere Kennwörter verwenden

Verwende sichere Kennwörter, die nicht im Wörterbuch zu finden sind, aus mindestens 8 Zeichen bestehen und mindestens drei der folgenden vier Zeichenarten beinhalten:

lateinische Großbuchstaben, lateinische Kleinbuchstaben, arabische Ziffern (0–9) und nicht-alphanumerische Zeichen.



DAS RISIKO

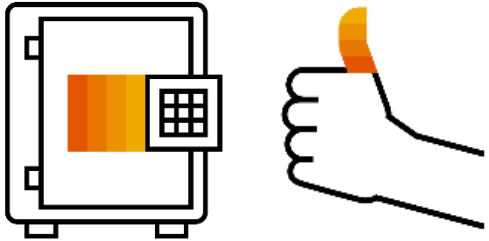
- ! Unbefugte können in Deinem Namen auf Unternehmensdaten zugreifen.
- ! Einfache oder kurze Kennwörter lassen sich einfach erraten oder knacken.

WAS KANN ICH TUN?

3. Kennwörter in Password Depot speichern

Lass nie Zettel mit Deinen Kennwörtern herumliegen. Speichere sie besser in Password Depot, einem Programm auf Deinem Computer.

Password Depot



DAS RISIKO

- Unbefugte können in Deinem Namen auf Unternehmensdaten zugreifen.
- Einfache oder kurze Kennwörter lassen sich einfach erraten oder knacken.

WAS KANN ICH TUN?

4. Für jedes System ein anderes Kennwort verwenden

Verwende für alle wichtigen Systeme, zum Beispiel Windows oder SAP, jeweils ein eigenes Kennwort.

Verwende Dein Windows-Kennwort nie für etwas anderes. Auch für Deine wichtigen privaten Konten solltest Du jeweils eigene Kennwörter verwenden.

Für jedes System ein anderes Kennwort

Kennwörter

Sehr gut! Du hast Folgendes gelernt:

1. Niemals Dein Kennwort verraten
2. Immer sichere Kennwörter verwenden
3. Kennwörter in Password Depot speichern
4. Für jedes System ein anderes Kennwort verwenden

Klassifizierung von Informationen

Aufgrund der Art unseres Geschäfts haben wir viel mit sensiblen Daten zu tun.

In diesem Teil lernst Du, wie Daten klassifiziert werden und wie man sie sorgfältig behandelt.

DAS RISIKO

- Informationen werden oft nicht richtig geschützt, weil sie entweder nicht oder falsch klassifiziert werden.
- In den falschen Händen können sensible Daten erheblichen Schaden anrichten.

Falsch oder gar nicht klassifizierte Informationen werden mit hoher Wahrscheinlichkeit falsch behandelt.

Wenn sensible Daten in die falschen Hände geraten, kann uns das beträchtlichen finanziellen Schaden zufügen und unseren Ruf beschädigen.

Deshalb ist es so wichtig, dass Daten korrekt klassifiziert und richtig behandelt werden.

DAS RISIKO

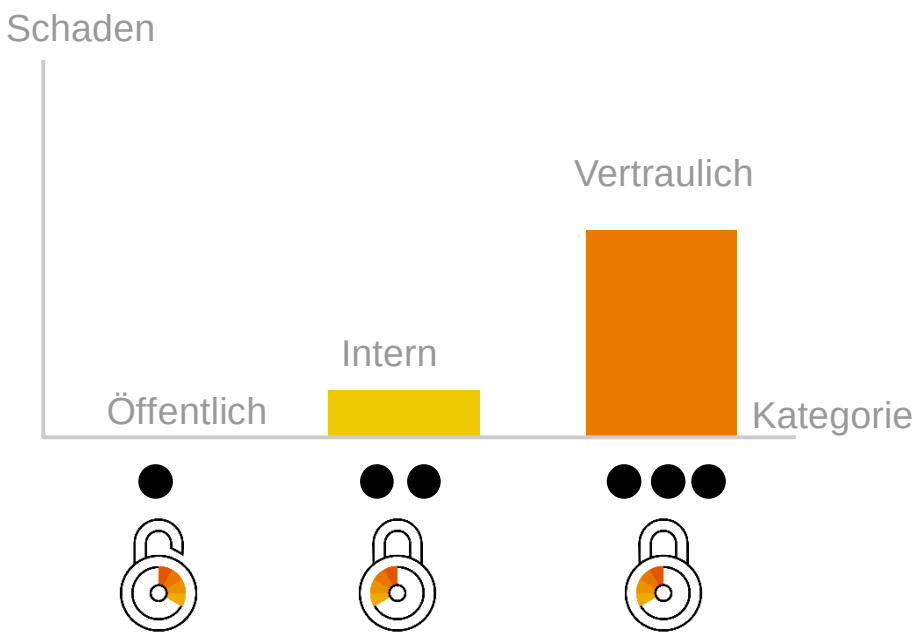
- Informationen werden oft nicht richtig geschützt, weil sie entweder nicht oder falsch klassifiziert werden.
- In den falschen Händen können sensible Daten erheblichen Schaden anrichten.

WAS KANN ICH TUN?

1. Informationen immer klassifizieren

Je mehr Schaden eine Information im Fall einer unberechtigten Weitergabe anrichten könnte, desto sensibler ist sie.

Klassifiziere und kennzeichne Daten immer entsprechend unseren Kategorien zur Informationsklassifizierung: Public (öffentlich), Internal (intern) und Confidential (vertraulich).



DAS RISIKO

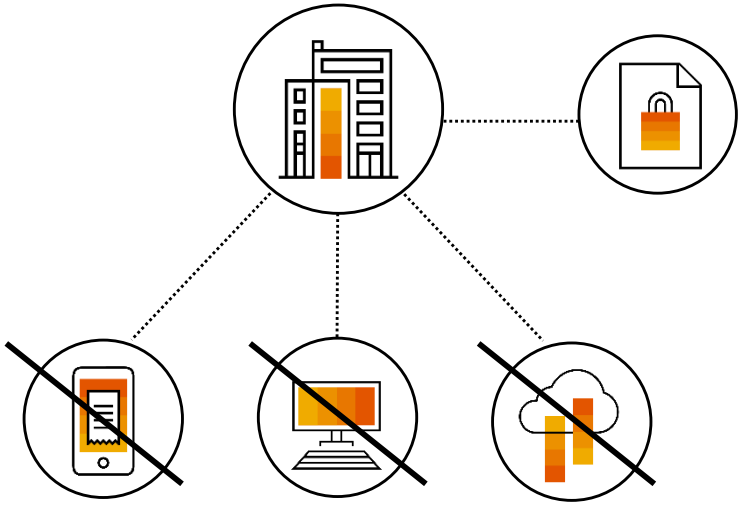
- Informationen werden oft nicht richtig geschützt, weil sie entweder nicht oder falsch klassifiziert werden.
- In den falschen Händen können sensible Daten erheblichen Schaden anrichten.

WAS KANN ICH TUN?

2 Am richtigen Ort ablegen

Sensible Daten sollten nur in der IT-Umgebung des Unternehmens gespeichert werden, die für diese Art von Informationen vorgesehen ist.

Speichere geschäftliche Daten nie auf einem privaten Computer oder auf einem privaten Cloud-Speicherplatz



DAS RISIKO

- Informationen werden oft nicht richtig geschützt, weil sie entweder nicht oder falsch klassifiziert werden.
- In den falschen Händen können sensible Daten erheblichen Schaden anrichten.

WAS KANN ICH TUN?

3 Sorgfältig behandeln

Kennzeichne die Daten immer entsprechend ihrer Vertraulichkeitsstufe.

Sperre digitale Daten an ihrem Speicherort und bewahre Daten in Papierform verschlossen auf.

Übertrage Daten nie unverschlüsselt.

Entsorge Daten ordnungsgemäß mit einem Aktenvernichter oder in einem gesicherten Behälter.

Dokumentklassifizierung: Confidential

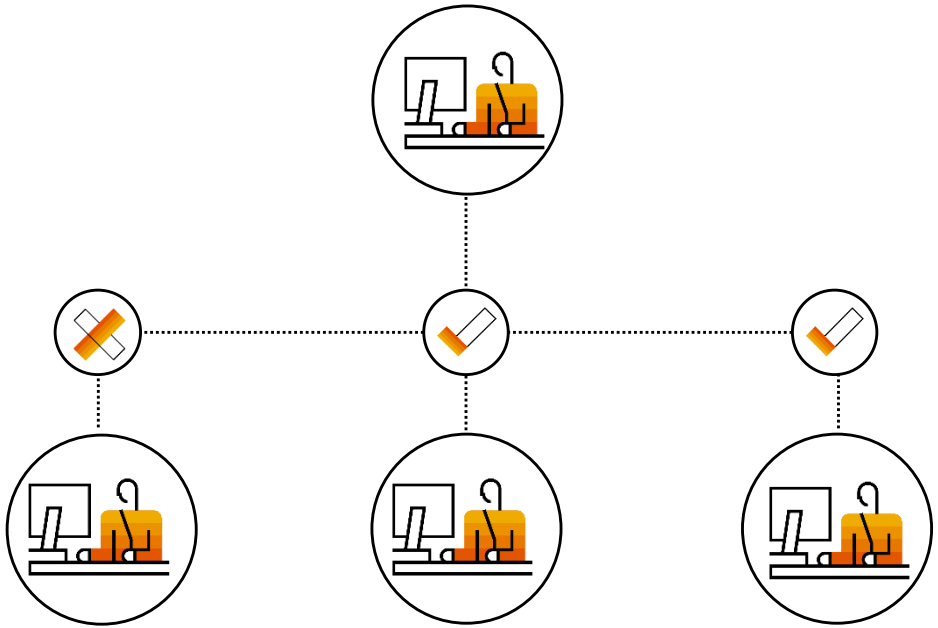
DAS RISIKO

- Informationen werden oft nicht richtig geschützt, weil sie entweder nicht oder falsch klassifiziert werden.
- In den falschen Händen können sensible Daten erheblichen Schaden anrichten.

WAS KANN ICH TUN?

4. Daten nur bei tatsächlichem Bedarf weitergeben

Gib an andere nur die Informationen weiter, die sie unbedingt benötigen, um ihre Aufgaben zu erledigen.



Klassifizierung von Informationen

Sehr gut! Du hast Folgendes gelernt:

1. Informationen immer klassifizieren
2. Am richtigen Ort ablegen
3. Sorgfältig behandeln
4. Daten nur bei tatsächlichem Bedarf weitergeben

Sicherer Arbeitsplatz

Informationen, die Du auf Deinem Schreibtisch liegen lässt, sind neugierigen Blicken und Langfingern ungeschützt ausgeliefert.

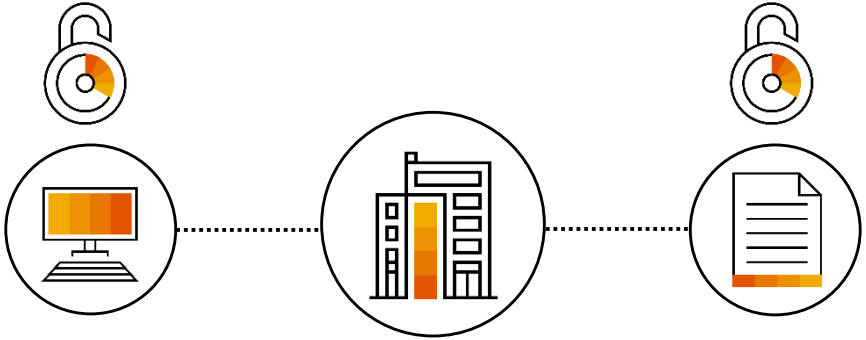
In diesem Teil lernst Du, wie man sensible und private Informationen schützt.

DAS RISIKO

! Es kann nie ausgeschlossen werden, dass Unbefugte unsere Geschäftsräume betreten. Dort können sie sich ganz einfach Zugang zu vertraulichen Informationen verschaffen.

Wir sind ein kunden- und gewinnorientiertes Unternehmen, nicht Fort Knox.

Angreifer finden immer eine Möglichkeit, unsere Gebäude zu betreten, und könnten dort ganz leicht auf herumliegende sensible Daten zugreifen.



DAS RISIKO

! Es kann nie ausgeschlossen werden, dass Unbefugte unsere Geschäftsräume betreten. Dort können sie sich ganz einfach Zugang zu vertraulichen Informationen verschaffen.

WAS KANN ICH TUN?

1 Vertrauliche Daten unter Verschluss halten

Schließe Dein Büro ab oder verschließe sensible Daten in einem Schrank, wenn Du Deinen Arbeitsplatz verlässt.

Sperre Deinen PC, auch wenn Du nur kurz weggehst.

An einem ungesperrten PC können Angreifer ganz einfach auf sensible Daten zugreifen oder Malware installieren.

odor

Mac users:

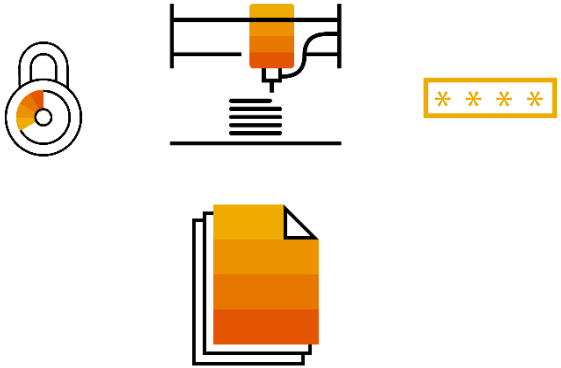
DAS RISIKO

! Es kann nie ausgeschlossen werden, dass Unbefugte unsere Geschäftsräume betreten. Dort können sie sich ganz einfach Zugang zu vertraulichen Informationen verschaffen.

WAS KANN ICH TUN?

2 Immer sicher drucken

Verwende zum Ausdrucken sensibler Daten immer die Technologie zum sicheren Drucken. Der Drucker beginnt erst mit dem Drucken, wenn Du Dich angemeldet hast.



DAS RISIKO

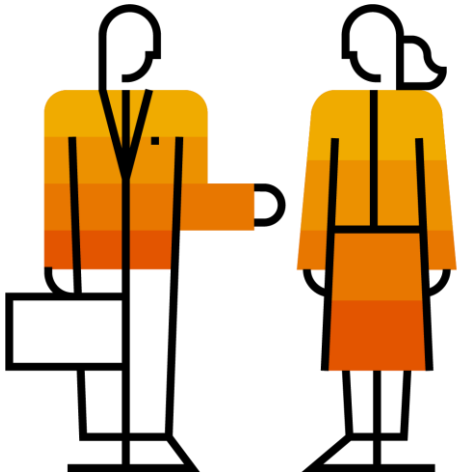
! Es kann nie ausgeschlossen werden, dass Unbefugte unsere Geschäftsräume betreten. Dort können sie sich ganz einfach Zugang zu vertraulichen Informationen verschaffen.

WAS KANN ICH TUN?

3 Besucher begleiten

Hole Besucher am Empfang ab und begleite sie wieder zum Ausgang oder zu ihrem nächsten Meeting. Sorge dafür, dass die Besucher ihren Besucherausweis sichtbar tragen.

Auch Du solltest Deinen Ausweis stets sichtbar tragen, wenn Du bei der SAP vor Ort bist.



DAS RISIKO

! Es kann nie ausgeschlossen werden, dass Unbefugte unsere Geschäftsräume betreten. Dort können sie sich ganz einfach Zugang zu vertraulichen Informationen verschaffen.

WAS KANN ICH TUN?

4 Vorfälle melden

Wenn Du einen Sicherheitsvorfall bemerkst, sei es ein physischer Verlust oder ein Einbruch, Hacking oder ein Social-Engineering-Angriff, melde ihn bitte sofort über unser Incident-Reporting-Tool.

Bei kritischen Vorfällen informierst Du bitte auch direkt das lokale Sicherheitsteam.

SICHERHEITSVORFALL

- Diebstahl oder Verlust von Geräten
- Offenlegung von Informationen
- Hacker- oder Malware-Angriffe
- Nicht autorisierter Zugriff auf IT-Systeme
- Körperlicher Schaden
- Und mehr

Quick Link: go/incident-reporting

Sicherer Arbeitsplatz

Sehr gut! Du hast Folgendes gelernt:

1. Vertrauliche Daten unter Verschluss halten
2. Immer sicher drucken
3. Besucher begleiten
4. Vorfälle melden

Phishing

Phishing ist der Versuch eines Hackers, sensible Daten abzugreifen oder sich dauerhaft Zugriff auf Deinen Computer zu verschaffen.

Das beginnt oft mit einer E-Mail, in der sich der Hacker als vertrauenswürdiger Absender ausgibt. In diesem Teil lernst Du, wie Du Phishing-Angriffe erkennen und Dich davor schützen kannst.

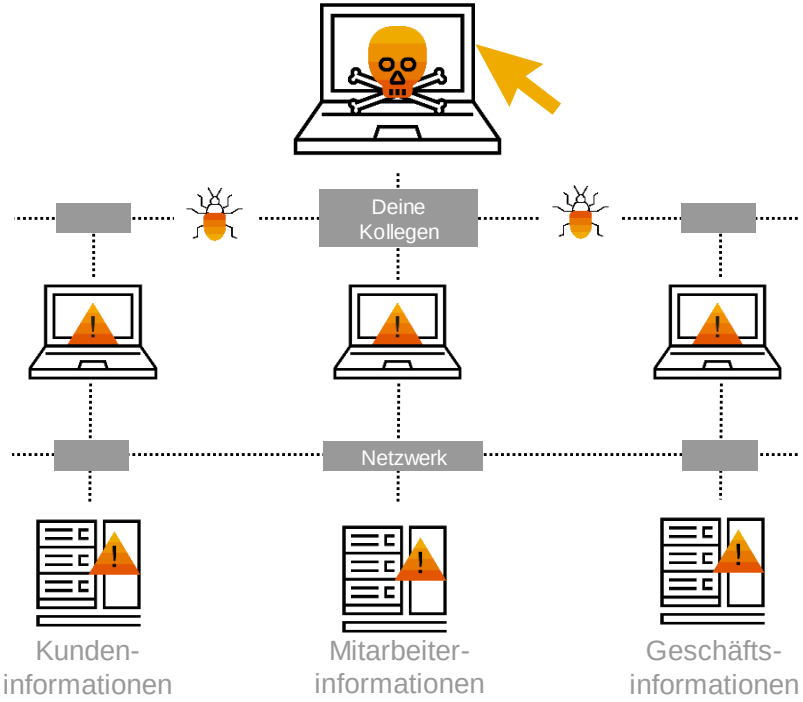
DAS RISIKO

Phishing-E-Mails können Infektionen auslösen, die unsere gesamte Unternehmens-IT beschädigen, und zum Verlust vertraulicher Informationen führen.

Wenn Du in Phishing-E-Mails auf Links oder Anhänge klickst, kann das System infiziert werden. Diese Infektionen können von Schadsoftware hervorgerufen werden, die unsere Virenschutzsoftware möglicherweise nicht erkennt.

Im schlimmsten Fall breitet sich die Infektion auf Deine Kollegen aus oder beschädigt gar unser gesamtes Netzwerk.

Das kann dazu führen, dass vertrauliche Informationen veröffentlicht werden, und enorme finanzielle Verluste sowie Rufschädigung zur Folge haben.



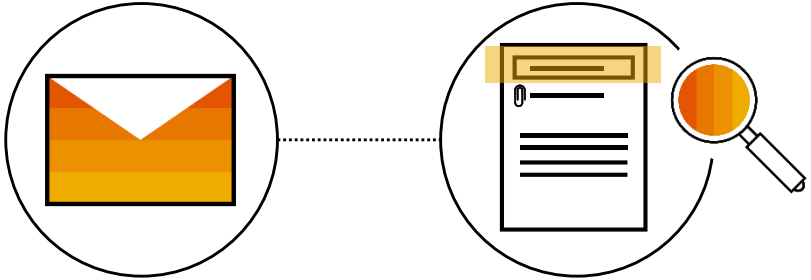
DAS RISIKO

! Phishing-E-Mails können Infektionen auslösen, die unsere gesamte Unternehmens-IT beschädigen, und zum Verlust vertraulicher Informationen führen.

WAS KANN ICH TUN?

1 E-Mail-Absender prüfen

Sieh nach, ob er in irgendeiner Weise verdächtig wirkt.



DAS RISIKO

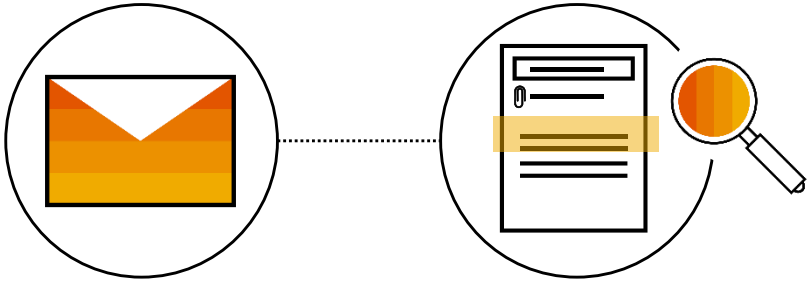
! Phishing-E-Mails können Infektionen auslösen, die unsere gesamte Unternehmens-IT beschädigen, und zum Verlust vertraulicher Informationen führen.

WAS KANN ICH TUN?

2 Anrede prüfen

Sieh nach, ob eine persönliche Anrede vorhanden ist.

Wirst Du mit Namen angesprochen?



DAS RISIKO

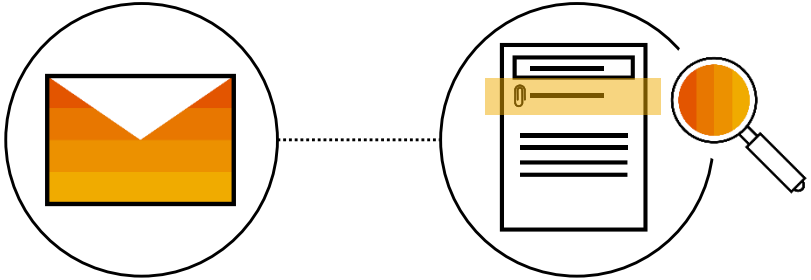
! Phishing-E-Mails können Infektionen auslösen, die unsere gesamte Unternehmens-IT beschädigen, und zum Verlust vertraulicher Informationen führen.

WAS KANN ICH TUN?

3 Links und Priorität prüfen

Phishing-E-Mails vermitteln fast immer eine gewisse Dringlichkeit und fordern Dich auf, auf einen Link zu klicken oder einen Anhang zu öffnen.

Wenn das verdächtig wirkt, klicke nicht auf den Link und öffne nicht den Anhang.



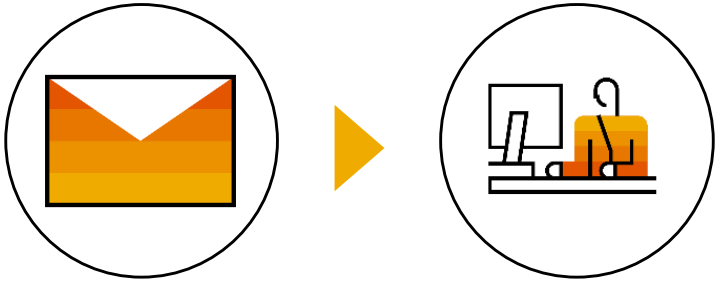
DAS RISIKO

! Phishing-E-Mails können Infektionen auslösen, die unsere gesamte Unternehmens-IT beschädigen, und zum Verlust vertraulicher Informationen führen.

WAS KANN ICH TUN?

4 Im Zweifel die Nachricht als Anhang an cybersecurity@sap.com senden

Wenn Du den Absender kennst, rufe ihn an und frage, ob er diese E-Mail tatsächlich gesendet hat.



cybersecurity@sap.com

Phishing

Sehr gut! Du hast Folgendes gelernt:

1. E-Mail-Absender prüfen
2. Anrede prüfen
3. Links und Priorität prüfen
4. Im Zweifel die Nachricht an cybersecurity@sap.com senden

Soziale Medien

Wir als Unternehmen haben nichts gegen soziale Netzwerke, solange Du Dich an unsere Regeln hältst.

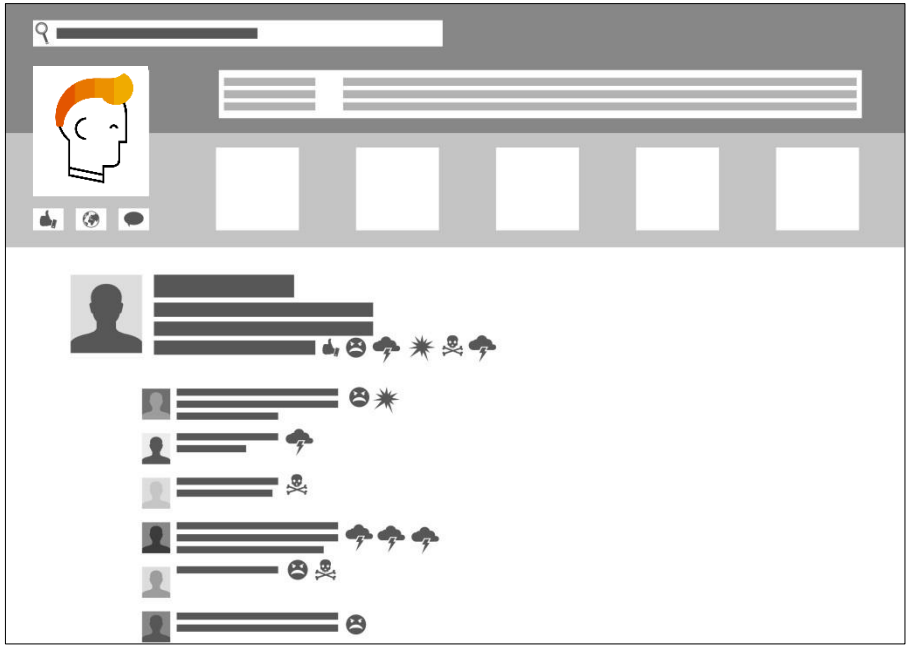
In diesem Teil lernst Du die wichtigsten Richtlinien für den Umgang mit sozialen Netzwerken kennen.

DAS RISIKO

- Der Ruf und das Image der SAP könnten beschädigt werden.
- Angreifer könnten sich wertvolle interne Informationen verschaffen.

Der Ruf eines Unternehmens kann durch unüberlegte Beiträge und Informationen in sozialen Netzwerken sehr schnell Schaden nehmen.

Außerdem durchsuchen professionelle Angreifer soziale Netzwerke nach wichtigen Informationen, die sie für einen Angriff missbrauchen könnten.



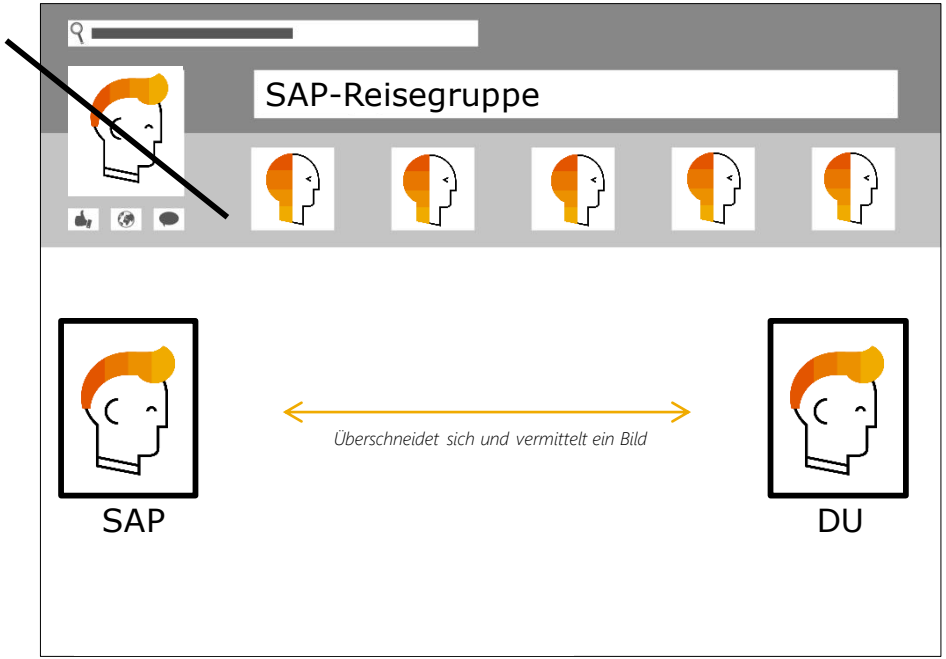
DAS RISIKO

- Der Ruf und das Image der SAP könnten beschädigt werden.
- Angreifer könnten sich wertvolle interne Informationen verschaffen.

WAS KANN ICH TUN?

1. Keine Nutzerprofile oder Gruppen im Namen der SAP einrichten

Richte nie Nutzerprofile oder Gruppen im Namen der SAP ein. Dafür ist unsere Kommunikationsabteilung zuständig.



DAS RISIKO

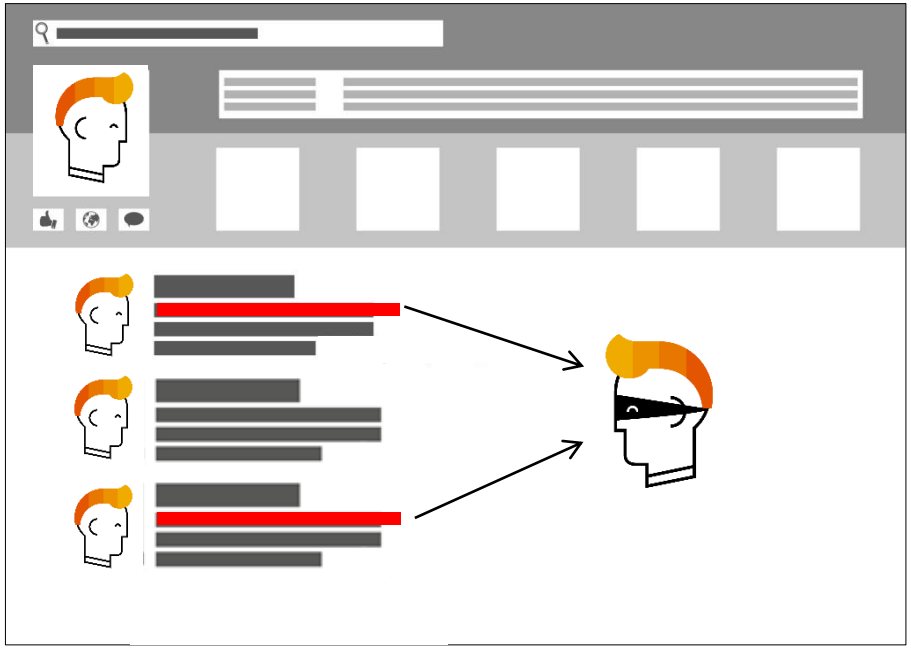
- Der Ruf und das Image der SAP könnten beschädigt werden.
- Angreifer könnten sich wertvolle interne Informationen verschaffen.

WAS KANN ICH TUN?

2 Keine internen Informationen weitergeben

Gib niemals interne oder vertrauliche Unternehmensinformationen weiter.

Auch harmlos scheinende Informationen, wie zum Beispiel Projektnamen oder welche Software eingesetzt wird, werden oft für gezielte Phishing- oder Social-Engineering-Angriffe missbraucht.



DAS RISIKO

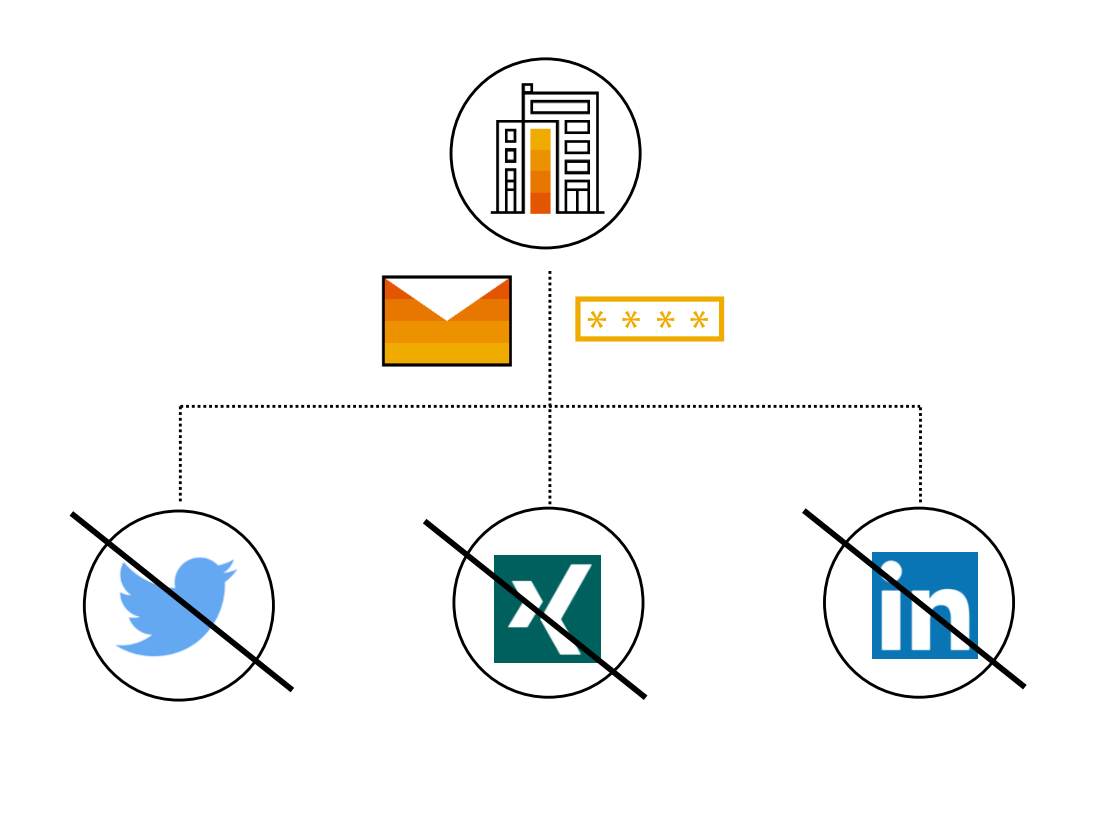
- Der Ruf und das Image der SAP könnten beschädigt werden.
- Angreifer könnten sich wertvolle interne Informationen verschaffen.

WAS KANN ICH TUN?

3. SAP-E-Mail-Adresse oder -Kennwörter nie außerhalb der Arbeit verwenden

Benutze Deine berufliche E-Mail-Adresse und Deine beruflichen Kennwörter niemals zum Anmelden in einem sozialen Netzwerk.

Wenn in dem sozialen Netzwerk eine Sicherheitslücke besteht, sind wir sonst auch gefährdet.



Soziale Medien

Sehr gut! Du hast Folgendes gelernt:

1. Keine Nutzerprofile oder Gruppen im Namen der SAP einrichten
2. Keine internen Informationen weitergeben
3. SAP-E-Mail-Adresse oder -Kennwörter nie außerhalb der Arbeit verwenden

Sichere Kommunikation

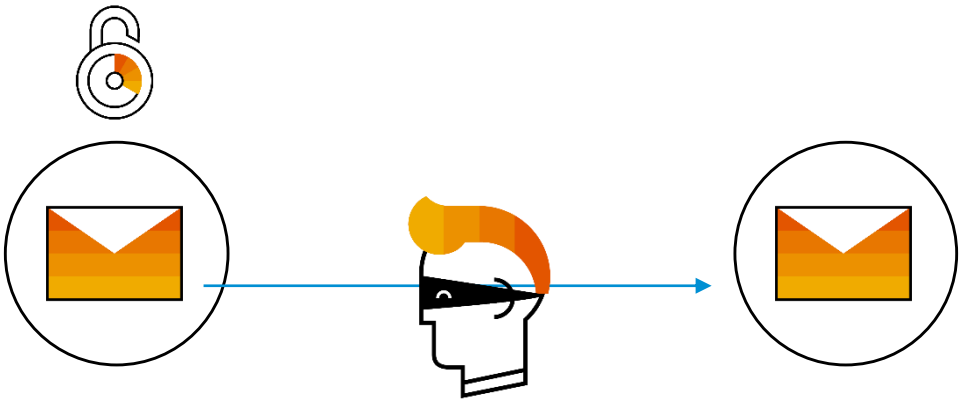
Wir alle müssen bei unserer täglichen Arbeit Informationen übertragen.

In diesem Teil lernst Du, wie das in Deinem Arbeitsumfeld auf sichere Weise geschieht.

DAS RISIKO

! Unverschlüsselte E-Mails und Public-Cloud-Speicherservices sind nicht sicher. Sensible Daten können verloren gehen oder in falsche Hände gelangen.

Wenn Du Informationen unverschlüsselt überträgst, zum Beispiel per E-Mail, sind diese vor fremden Blicken genauso wenig geschützt wie eine Postkarte.



DAS RISIKO

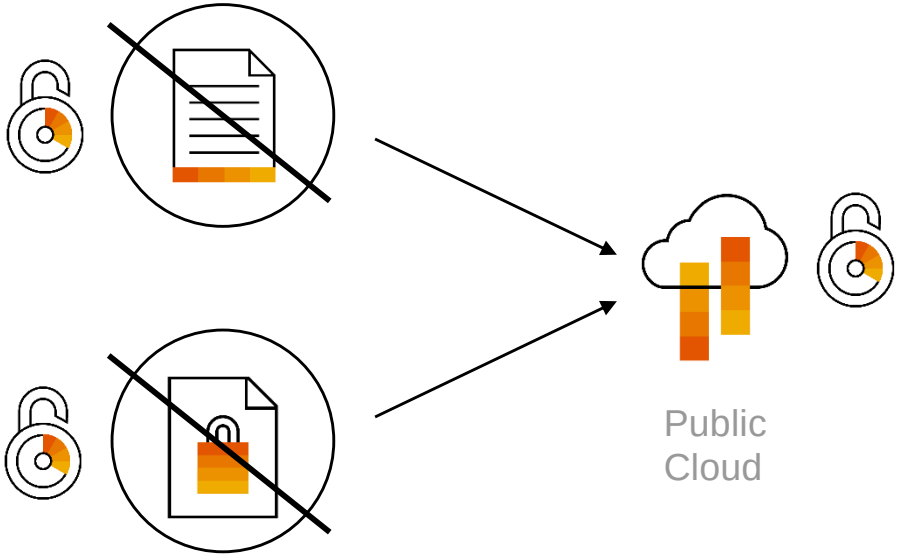
! Unverschlüsselte E-Mails und Public-Cloud-Speicherservices sind nicht sicher. Sensible Daten können verloren gehen oder in falsche Hände gelangen.

WAS KANN ICH TUN?

1 Keine nicht autorisierten Cloud-Services nutzen

Unsere Geschäftsinformationen müssen immer in der IT-Umgebung unseres Unternehmens bleiben. Gelangen Daten nach draußen, werden sie angreifbar. Wir haben dann keinerlei Kontrolle mehr über sie.

Verwende deshalb für Geschäftsdaten niemals Cloud-Services, die **nicht autorisiert** sind.



DAS RISIKO

! Unverschlüsselte E-Mails und Public-Cloud-Speicherservices sind nicht sicher. Sensible Daten können verloren gehen oder in falsche Hände gelangen.

WAS KANN ICH TUN?

2 Genehmigte Tools verwenden

Verwende für den Austausch von Geschäftsdaten nur von SAP genehmigte Lösungen wie OneDrive for Business.

Mit vielen davon kannst Du sogar vertrauliche Informationen übertragen.

- SharePoint Online
- OneDrive for Business
- SAP Jam
- Und mehr

Quick Link: https://go.sap.corp/exchanging-confidential-data

DAS RISIKO

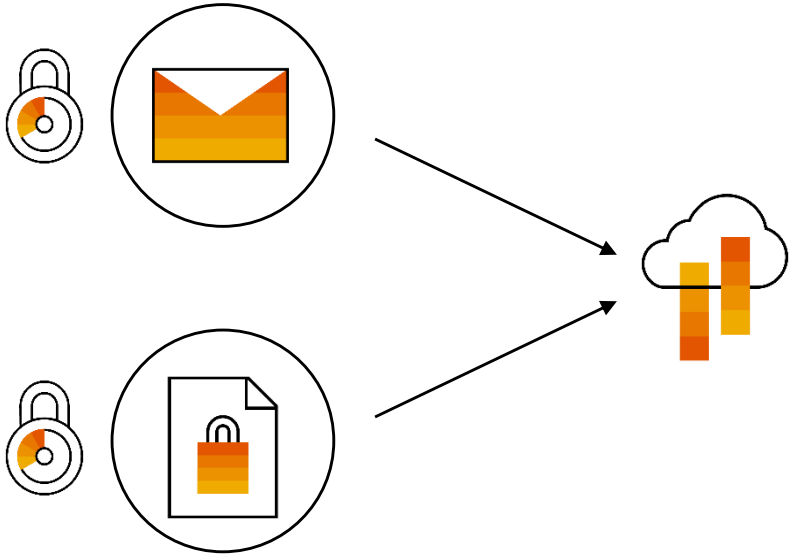
! Unverschlüsselte E-Mails und Public-Cloud-Speicherservices sind nicht sicher. Sensible Daten können verloren gehen oder in falsche Hände gelangen.

WAS KANN ICH TUN?

3 Sensible Daten immer verschlüsseln

Weil unverschlüsselte Informationen von vielen Menschen gelesen werden können, musst Du sensible Daten immer verschlüsselt übertragen.

Wenn Du Deine E-Mails verschlüsseln kannst, dann tue das bitte. Falls nicht, kannst Du vertrauliche Anhänge in einer ZIP-Datei verschlüsseln oder ein genehmigtes sicheres Tool für den Datenaustausch nutzen.



DAS RISIKO

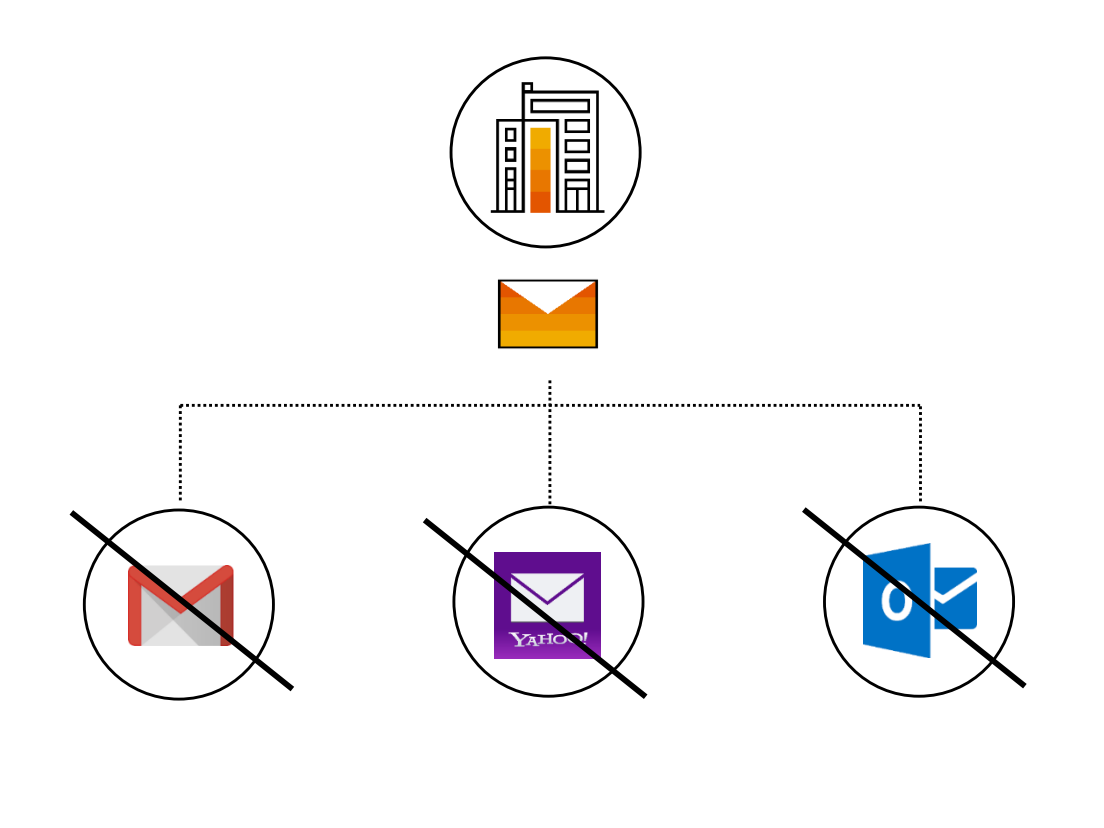
! Unverschlüsselte E-Mails und Public-Cloud-Speicherservices sind nicht sicher. Sensible Daten können verloren gehen oder in falsche Hände gelangen.

WAS KANN ICH TUN?

4 Keine persönlichen E-Mail-Konten verwenden

Bitte benutze für unsere Geschäftsdaten auch keine privaten E-Mail-Konten, und richte keine automatische Weiterleitung auf private Konten ein.

Dort würden die Daten unverschlüsselt übertragen, und der private Client könnte mit Malware infiziert sein.



Sichere Kommunikation

Sehr gut! Du hast Folgendes gelernt:

1. Keine nicht autorisierten Cloud-Services nutzen
2. Genehmigte Tools verwenden
3. Sensible Daten immer verschlüsseln
4. Keine persönlichen E-Mail-Konten verwenden

Compliance

Jeder Mensch, der für die SAP tätig ist, muss sich dessen bewusst sein, dass Werte wie Ehrlichkeit, Integrität, Transparenz, Vertrauenswürdigkeit und Verantwortungsgefühl die Grundlage für alle geschäftlichen Tätigkeiten bilden sollen.

In diesem Abschnitt lernen Sie, inwiefern die Geschäftsgrundsätze für externe Mitarbeiter (Code of Business Conduct for External Workers, „CoBC“) dem Ziel dienen, Risiken zu minimieren und Ihnen helfen, Interessenkonflikte zu vermeiden, unzulässige Aktivitäten wie etwa Bestechung auszuschließen und das Richtige zu tun, um bei der Ausführung Ihrer Aufgaben für die SAP die Einhaltung aller Gesetze sicherzustellen.

Zielsetzung und Geltungsbereich

Geschäftsgrundsätze für externe Mitarbeiter:

- Regeln **Verhaltensstandards** für den Umgang mit allen wirtschaftlichen, juristischen und ethischen Herausforderungen des Geschäftsalltags.
- Sollen **Maßstab und Orientierungshilfe** sowohl für die Zusammenarbeit mit Kunden, Lieferanten und Partnern sein als auch für das Verhalten gegenüber Wettbewerbern und für Aktivitäten im finanziellen Bereich, u. a. auch für Transaktionen mit SAP-Aktien.
- Diese Grundsätze gelten **ohne Ausnahme** für **alle externen Mitarbeiter**, die für bzw. im Namen von Unternehmen des SAP-Konzerns arbeiten, u. a. Tochtergesellschaften, übernommene und verbundene Unternehmen, Niederlassungen und Repräsentanzen der SAP.

Definitionen (I)

„Externer Mitarbeiter“ ist eine einzelne, **nicht bei der SAP fest angestellte Person**, die:

- für die SAP und/oder im Namen der SAP arbeitet,
  - unabhängig davon, ob sie intern von der SAP (nicht abrechenbar) oder bei einem Kundenprojekt (abrechenbar) eingesetzt wird,
  - unabhängig davon, ob sie vor Ort oder remote tätig ist,
  - auch wenn sie nur Systemzugriff benötigt.

Definitionen (II)

„Externe Mitarbeiter“ sind **typischerweise** (aber nicht nur):

- Leiharbeitskräfte (Zeitpersonal),
- Projektdienstleister,
- Dienstleister für ausgelagerte Dienstleistungen,
- Partner, die Testaktivitäten unterstützen,
- Diplomanden, Doktoranden.

Einhaltung der Gesetze

Während der Tätigkeit für die SAP als externer Mitarbeiter sind alle Geschäftsaktivitäten für die SAP bzw. im Auftrag der SAP **in vollständiger Übereinstimmung <u>mit allen geltenden</u> Gesetzen, Vorschriften, Bestimmungen und Richtlinien auszuüben**, insbesondere mit

- Korruptionsbekämpfungsgesetzen
- Kartell- und Wettbewerbsrecht
- Wertpapierhandelsgesetzen und Gesetzen gegen Insiderhandel
- Datenschutzgesetzen
- Markenrecht und Urheberrecht

Interessenkonflikte (I)

- Wer für die SAP arbeitet, muss die Interessen der SAP jederzeit wahren.
- Geschäftschancen für die SAP dürfen nicht zu Ihrer persönlichen Vorteilsnahme oder zum Vorteil von Verwandten, Freunden oder Ihres eigenen Unternehmens missbraucht werden.
- Eigene Produkte oder Produkte von Dritten dürfen nicht entwickelt oder verkauft werden, und Dienstleistungen dürfen nicht erbracht werden, wenn die SAP ähnliche Produkte oder Dienstleistungen anbietet.
- Bestehende Interessenkonflikte müssen offengelegt und – wenn möglich – begrenzt werden, damit sie sich nicht auf Geschäftsbeziehungen und/oder Geschäfte (Verträge) auswirken.

Interessenkonflikte (II)

Beispiel:

Der externe Mitarbeiter X ist bei einem SAP-Projekt an der Vorbereitung eines Angebots bzw. Verkaufsgesprächs für Kunde Y beteiligt.

X ist zufällig der Schwiegersohn des Geschäftsführers von Kunde Y. Er beeinflusst das Verkaufsgespräch durch die Kenntnisgabe vertraulicher Informationen, dank derer die SAP den Zuschlag erhält.

- RISIKO: Verstoß gegen Ausschreibungsregeln. Je nach der lokalen Gesetzgebung kann X persönlich haftbar gemacht werden, und gegen die SAP könnten Ermittlungen eingeleitet werden.

Bestechung und Korruption (I)

- **Keine Korruption** – Entscheidungsträger dürfen nicht durch persönliche Vorteile dazu bewogen werden, Entscheidungen zugunsten der SAP zu treffen.
- **Keine Bestechung** – Nehmen Sie keine persönlichen Vorteile als Gegenleistung für eine Entscheidung zugunsten der SAP an.
- **Keine persönlichen Vorteile für Regierungsvertreter/Beamte („Government/Public Officials“).**
- Die SAP vermeidet **auch nur den Anschein** von unethischem Verhalten.

Bestechung und Korruption (II)

Beispiel:

Der externe Mitarbeiter X ist an einem SAP-Projekt zur Entwicklung innovativer Lösungen und Strategien für die Digitalisierung einer Stadtverwaltung beteiligt. Um das Projekt voranzubringen und die Stadt dazu zu bewegen, weitere Software zu kaufen, beschließt X, den Bürgermeister zu einem Fußballspiel einzuladen, um mit ihm in entspannter Atmosphäre über die Vorteile von SAP-Lösungen zu sprechen.

- RISIKO: Jeglicher Vorteil, der einem Beamten gewährt wird, stößt bei den Behörden auf Misstrauen. Das Einladen des Bürgermeisters – eines **Beamten** – zu dem Fußballspiel könnte in diesem Kontext als Bestechungsversuch aufgefasst werden. Das könnte für X strafrechtliche Folgen haben.

Bewirtung und Geschenke (I)

Als **Bewirtung** gelten Veranstaltungen, bei denen die Unterhaltung im Vordergrund steht (weniger als 80 % der Aktivitäten sind geschäftlicher Natur). Einladungen zu solchen Veranstaltungen unterliegen strengen, verbindlichen Compliance-Regeln, die strafbare Handlungen unterbinden und ethisches Verhalten fördern sollen. Diese Regeln gelten auch für externe Mitarbeiter.

- Beamte
  - Es ist streng verboten, Regierungsvertreter/Beamte („Government/Public Officials“) zu Bewirtungsveranstaltungen einzuladen.
  - Unter „Beamte“ werden dabei alle Personen verstanden, deren Arbeit vom Steuerzahler finanziert wird. Dazu zählen neben den eigentlichen Beamten auch Mitarbeiter staatseigener oder staatlich geleiteter Firmen (oft in den Bereichen Luftfahrt und Verteidigung, Versorgungswirtschaft, Energie- und Rohstoffindustrie, Telekommunikation und Transport), militärisches Personal, gewählte oder ernannte Funktionäre und Mitarbeiter internationaler Organisationen wie der Weltbank.

Bewirtung und Geschenke (II)

➢ <u>Ausschreibungsverfahren (Verkaufszyklus)</u>

- Keine Bewirtungsveranstaltungen für Kunden oder Lieferanten, wenn wir uns in Vertragsverhandlungen befinden, bei denen die SAP auf der Käufer- oder Verkäuferseite steht.

- Gleiches gilt für Verträge, die die SAP erst kürzlich geschlossen hat oder in Kürze schließen wird (3-Monats-Frist vor und nach dem Vertragsschluss).

- Die lokal geltenden Grenzen für die Bewirtung dürfen nicht überschritten werden.

Bewirtung und Geschenke (III)

- Die Bewirtungsregeln gelten auch für externe Mitarbeiter.
- Vor einer Teilnahme an einer Bewirtungsveranstaltung müssen Sie sich im Voraus mit Ihrem Ansprechpartner bei der SAP abstimmen.
- Sie dürfen erst dann zu einer Bewirtungsveranstaltung (dazu gehören auch Mittag- und Abendessen) einladen, wenn Sie die erforderliche schriftliche Freigabe bzw. Genehmigung von Ihrem Ansprechpartner bei der SAP, dem Field Compliance Officer und dem CFO der betreffenden Tochtergesellschaft erhalten haben.

Bewirtung und Geschenke (IV)

Geschenke

- Geschenke und Zuwendungen von externen Mitarbeitern an Dritte sind nicht erlaubt.
- Die SAP leistet grundsätzlich keine Geld- und Sachspenden für parteipolitische Zwecke. Wenn Sie als externer Mitarbeiter in Ihrem privaten Bereich eine solche Spende leisten, dürfen Sie nicht den Eindruck entstehen lassen, die Spende würde im Zusammenhang mit der SAP stehen.

Bewirtung und Geschenke (V)

- Diese Regeln sollen Sie nicht in Ihrer persönlichen Lebensführung einschränken.
- Wenn Sie an einem SAP-Auftrag arbeiten, können Sie jedoch als Vertreter der SAP wahrgenommen werden. Deshalb müssen wir von vornherein Situationen vermeiden, die missverstanden werden könnten.

Bewirtung und Geschenke (VI)

Beispiel:

Cyberland GmbH möchte neue Software anschaffen und steht mit mehreren Softwareunternehmen in Verhandlung. Der externe Mitarbeiter X gehört zu einem SAP-Team, das mit Cyberland verhandelt. Um die Verhandlungen voranzubringen und Cyberland GmbH dazu zu bewegen, Software von der SAP zu kaufen, beschließt X, den Geschäftsführer von Cyberland GmbH zu einem Fußballspiel einzuladen. X möchte das Fußballspiel nutzen, um mit dem Geschäftsführer in entspannter Atmosphäre über die Vorteile von SAP-Lösungen zu sprechen.

- RISIKO: Das Einladen des Geschäftsführers von Cyberland zu einem Fußballspiel während eines laufenden **Ausschreibungsverfahrens/Verkaufszyklus** könnte in diesem Kontext als Versuch der Einflussnahme aufgefasst werden. Das könnte für X strafrechtliche Folgen haben.

Vertraulichkeit (I)

- Alle internen betrieblichen Unterlagen, Daten, Dateien, Aufzeichnungen und Berichte, die im Rahmen der Tätigkeit für die SAP erworben oder erstellt wurden, sind Eigentum der SAP und gelten als vertrauliche Informationen.
- Insbesondere Informationen zu Preisen, zur Entwicklung von Produkten und Dienstleistungen sowie Geschäftsgeheimnisse sind streng vertraulich zu behandeln.
- Der Austausch von vertraulichen Informationen mit SAP-Kunden, -Lieferanten und -Partnern ist verboten, ebenso wie die Annahme von vertraulichen Informationen von SAP-Kunden, -Lieferanten und -Partnern.

Vertraulichkeit (II)

- Externe Mitarbeiter nehmen nicht aus eigener Initiative Kontakt zu Vertretern der Medien oder der Finanzwelt auf.
- Die Nutzung von SAP-E-Mail-Konten für private Zwecke ist verboten.
- Externe Mitarbeiter haben die Möglichkeit, auf das Internet zuzugreifen, sofern dies keine unberechtigte Verwendung urheberrechtlich geschützter Materialien und keinen unerlaubten Zugriff auf vertrauliche Informationen, Quellcode oder Produkte von Wettbewerbern darstellt.

Verhalten gegenüber Kunden

- Vertragsänderungen dürfen nicht ohne Genehmigung der Rechtsabteilung vereinbart werden.
- Vereinbarungen über Boykotte gegen Kunden, Lieferanten, Wettbewerber, Partner oder Dienstleister sind rechtswidrig.
- Exklusivverträge würden den Wettbewerb auf dem Markt beeinträchtigen und sind deshalb rechtswidrig.
- Externe Mitarbeiter der SAP sorgen dafür, dass die SAP keine Geschäfte auf Gegenseitigkeit abschließt, wonach die SAP Produkte oder Dienstleistungen eines anderen Unternehmens nur dann abnimmt, wenn dieses Unternehmen Produkte der SAP bezieht.

Verhalten gegenüber Lieferanten

- Externe Mitarbeiter zwingen Lieferanten nicht, als Gegenleistung für Einkäufe von SAP ihrerseits SAP-Produkte zu kaufen.
- Die SAP darf aber, genau wie bei jedem anderen Kunden, unabhängig von einer Bestellung versuchen, Produkte an ihre Lieferanten zu verkaufen.

Verhalten gegenüber Wettbewerbern

- Jede Form von Preisabsprachen zwischen Wettbewerbern ist verboten.
- Alle Formen der Absprache zwischen Wettbewerbern in Verbindung mit einer geheimen vorherigen Abmachung, wer für einen über ein Ausschreibungsverfahren zu vergebenden Auftrag das beste Angebot abgibt („Angebotsabsprachen“, „BidRigging“), sind strengstens verboten.
- Bei Kontakten zu Wettbewerbern sprechen externe Mitarbeiter der SAP nicht über interne Angelegenheiten der SAP, aus denen Wettbewerber Wettbewerbsvorteile gegenüber der SAP ziehen könnten.
- Externe Mitarbeiter der SAP versuchen auf keinen Fall, mit unlauteren Mitteln Geschäftsgeheimnisse oder andere vertrauliche oder geheime Informationen eines Wettbewerbers zu erlangen, anzunehmen, zu lesen oder zu verwenden.

Verhalten gegenüber Partnern

- Vertragsänderungen dürfen nicht ohne Genehmigung der Rechtsabteilung vereinbart werden.

- Externe Mitarbeiter vermeiden alle Formen der einseitigen Bevorzugung eines bestimmten Partners. Dies gilt insbesondere auch bei konkurrierenden Angeboten mehrerer Partner für ein und denselben Kunden.

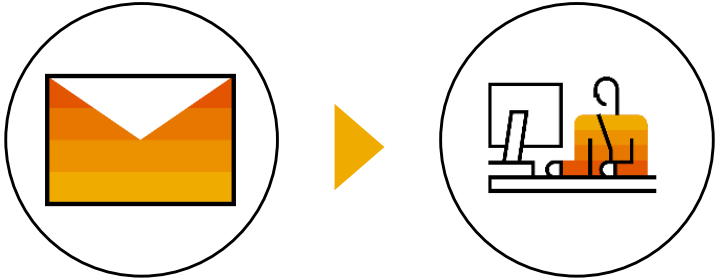
MELDUNGEN

! Zweifel oder Fragen hinsichtlich Verstößen gegen die Geschäftsgrundsätze sind von den externen Mitarbeitern zu melden.

WAS KANN ICH TUN?

Bei Fragen, Problemen oder Bedenken wenden Sie sich bitte an das Legal Compliance & Integrity Office (LCIO).

Kontakt:
global-compliance-office@sap.com
oder +49 6227 7 40022



global-compliance-office@sap.com

Rufnummer:
+49 6227 7 40022

Compliance

Sehr gut! Jetzt haben Sie Wissen über Folgendes:

1. Die Ziele und den Geltungsbereich der Geschäftsgrundsätze.
2. Wie Sie die Gesetze einhalten.
3. Wo Interessenkonflikte auftreten können.
4. Dass die SAP Bestechung und Korruption, gleich welcher Art, unter keinen Umständen duldet.
5. Wann Informationen als vertraulich zu behandeln sind.
6. Wie Sie sich gegenüber Kunden, Lieferanten, Wettbewerbern und Partnern verhalten müssen.
7. Dass Sie sich mit Fragen, Problemen und Bedenken an das LCIO wenden können.

Teste Dein Wissen!

Dir werden 16 Fragen gestellt. Du musst mindestens 11 der 16 Fragen richtig beantworten, um die Schulung zu bestehen. Frage 16 ist verpflichtend und kann nicht ausgelassen werden

Viel Erfolg!

START THE TEST