# FRAGEN-SAMMLUNG

## für eine interne Security Umfrage

Data Security Guide

# Fragensammlung für eine interne Security Umfrage

Nutzen Sie diese Beispielfragen als Hilfsmittel zur Erstellung Ihrer eigenen unternehmensinternen Sicherheitsumfrage. **Ergänzt und angepasst an Ihre Unternehmensspezifika**, können sie Ihnen helfen, zu überprüfen, ob der gewünschte Kenntnisstand erreicht ist oder doch noch Lücken vorhanden sind.

**1. Was solltest Du im Falle einer Veröffentlichung des Firmenpasswortes tun? (Mehrfachantworten möglich)**

a) Nichts.
b) Sofort das Passwort ändern.
c) Die Situation als einen Sicherheitsvorfall melden.
d) Warten, ob etwas passiert.

**Richtige Antworten: b), c)**

Begründung: Wie in der Richtlinie zur Informationssicherheit (*bitte fügen Sie einen Verweis auf Ihre Sicherheitsrichtlinien ein*) beschrieben, muss der Mitarbeiter im Falle der Offenlegung eines Passworts das Passwort sofort ändern und den Sicherheitsvorfall melden.

**2. Was ist das sichere Verfahren bei Verlust eines Zugriffstokens, Schlüssels oder Chipkarte?**

a) Betreten des Firmengeländes ohne Verifizierung in Begleitung eines Mitarbeiters oder mit dessen Schlüsselkarte.
b) Warte eine Weile (z.B. eine Woche) und wenn danach nicht wiedergefunden, melde den Verlust.
c) Melde den Verlust unverzüglich.
d) Beantrage einen Gästeausweis und verwende diesen stattdessen.

**Richtige Antwort: c)**

Begründung: Es ist ungemein wichtig eine verlorene Schlüsselkarte sofort zu melden, sodass diese gesperrt werden kann, um möglichen Missbrauch zu verhindern.

**3. Wie kann ich die Vertraulichkeit sensibler Daten schützen, die per E-Mail verschickt werden?**

a) Ich füge am Ende der Mail eine Vertraulichkeitsklausel an.
b) Gar nicht, weswegen ich keine sensiblen Daten per E-Mail versende.
c) Ich verschlüssele die E-Mail.
d) Ich signiere die E-Mail.

**Richtige Antwort: c)**

Begründung: Deine E-Mail-Nachrichten können von einem Angreifer abgefangen werden, entweder während sie auf dem E-Mail-Server gespeichert sind oder während sie sich über das Internet bewegen. Die digitale Signatur beweist dem Empfänger, dass Du den Inhalt der Nachricht signiert hast und dass der Inhalt während der Übertragung nicht verändert wurde, aber sie macht die Nachrichten nicht unlesbar. Die Verschlüsselung macht Nachrichten von dem Punkt, an dem sie ihre Reise beginnen, bis zu dem Punkt, an dem der beabsichtigte Empfänger sie öffnet, unlesbar. Du kannst Verschlüsselungsfunktionen verwenden, die auf digitalen Zertifikaten basieren, die im E-Mail-Dienst enthalten sind, oder andere verfügbare Verschlüsselungssoftware (z.B. PGP/GPG) herunterladen.

**4. Wie kann es zur Infektion Deines Computers mit Malware kommen? (Mehrfachantworten möglich)**

a) Durch Ausführen von Malware, die als legitimes Programm getarnt ist.
b) Durch den Besuch einer infizierten Webseite.
c) Durch E-Mails in HTML und/oder Anhänge (MS Office, PDF).
d) Durch Verbindung zu einem infizierten Netzwerk – Hotel, Zug, Bus, kostenloser Wi-Fi Hotspot.

**Richtige Antworten: a), b), c), d)**

Begründung: Die Verbreitung von schädlichem Code durch Tarnen der Schadsoftware als legitimes Programm oder mobile Applikation ist ein bekannter Infektionsweg. Aber auch der Besuch einer infizierten Webseite, die Infektion per E-Mail oder das Anschließen eines Geräts an ein infiziertes Netzwerk stellen eine Gefahr dar.

**5. Wie kann man das Risiko von Spam im beruflichen E-Mail-Postfach reduzieren? (Mehrfachantworten möglich)**

a) Die berufliche E-Mail-Adresse nicht für die Anmeldung bei Diensten nutzen, die keinen Bezug zum Arbeitsauftrag haben.
b) Die berufliche E-Mail-Adresse in öffentlichen Foren posten.
c) Sich nur bei seriösen Newslettern registrieren.
d) Die berufliche E-Mail Adresse ausschließlich für Aktivitäten mit Arbeitsbezug verwenden.

**Richtige Antworten: a), c), d)**

Begründung: Wenn Du so wenig wie möglich Spam in Deinem beruflichen E-Mail-Postfach haben möchtest, sollten Du behutsam bei der Verwendung Deiner beruflichen E-Mail-Adresse sein. Das gilt insbesondere auf öffentlichen Webseiten, wie Foren oder sozialen Netzwerken aber auch für geschlossene Chats. Wenn Du E-Mail für private Zwecke nutzen möchtest, darfst Du Deine berufliche E-Mail-Adresse dafür nicht nutzen. Auf E-Mails solltest Du nur antworten, wenn Du diese auch für vertrauenswürdig hältst. Wenn eine Nachricht oder deren Absender verdächtig oder nicht vertrauenserweckend sind, lasse die Legitimität der E-Mail durch die IT oder IT-Security Abteilung überprüfen. Vorsicht gilt auch für das (vermeintliche) Abmelden von E-Mail-Verteilern. Die Antwort auf Spam bestätigt dem Spammer nur, dass die E-Mail-Adresse aktiv ist.

**6. Welche der folgenden Aktionen hilft Dir Dein Endgerät vor Malware und Viren zu schützen?**

a) Software nur von vertrauenswürdigen Quellen beziehen.
b) Ein Antiviren-Programm installieren.
c) System-Updates schnellstmöglich installieren.
d) Alle obenstehenden Optionen.

**Richtige Antwort: d)**

Begründung: Alle auswählbaren Optionen verringern das Risiko von Problemen mit Viren/Malware.

**7. Wo sollten sich Firmengeräte (Laptops, Monitore), mit denen Daten der Kategorie „VERTRAULICH“ oder „STRENG VERTRAULICH“ bearbeitet werden, befinden?**

a) Das ist unwichtig.
b) In der Nähe eines Fensters.
c) In der Nähe einer Tür.
d) Dort, wo unautorisierte Personen keine Sicht auf die vertraulichen Daten haben.

**Richtige Antwort: d)**

Begründung: Geräte, die als „vertraulich“ oder „streng vertraulich“ eingestufte Daten verarbeiten, sollten so platziert werden, dass lediglich ein minimales Risiko der Einsicht solcher Daten durch Unbefugte besteht.

**8. Welche Regeln/Welches Verhalten muss man bei der Nutzung von Firmensmartphones einhalten? (Mehrfachantworten möglich)**

a) Die Richtlinien für Passwörter und zum Sperren der Geräte
b) Verschlüsselung der Geräte und der Speicherkarten
c) Beliebige, verfügbare Apps installieren
d) Alles oben Erwähnte

**Richtige Antwort: a), b)**

Begründung: Die Richtlinien für Mobilgeräteverwaltung und praxiserprobte Maßnahmen empfehlen, die Daten auf dem Handy vor nicht autorisiertem Zugriff zu schützen. Dies geschieht durch:

- Richtlinien zur Sperrung und Richtlinien zu Passwörtern
- Verschlüsselung des Inhaltes des Handys (und der Karte, wenn vorhanden)

Gleichzeitig muss die Appinstallation von außerhalb vertrauenswürdiger Quellen unterbunden werden. Zu vertrauenswürden Quellen gehören iTunes, Google Play und MDM Market.

**9. Du besuchst eine Webseite über ein öffentliches WLAN, allerdings ist Dein Antiviren-Programm nicht auf dem aktuellen Stand. Welche der folgenden Behauptungen ist wahr?**

a) Das Gerät ist nach wie vor nicht in Gefahr, da Du nur Websites mit Nachrichten aus Deinem Land besuchst.
b) Die Kommunikation über das HTTP-Protokoll kann nicht abgehört werden.
c) Die Kommunikation zu Firmenressourcen via VPN ist sicher.
d) Keine der oben genannten Behauptungen ist wahr.

Richtige Antwort: d)

Begründung: HTTP ist ein Kommunikationsprotokoll, über das sich der Webserver und Browser miteinander verständigen. Dieses Protokoll ist nicht in der Lage die Vertraulichkeit der übertragenen Daten zu wahren. Es ist somit möglich sie abzuhören. Eine Infektion des Computers ist auch beim gewöhnlichen Surfen auf legitimen Webseiten möglich und die Wahrscheinlichkeit der Infektion ist höher, wenn das Antiviren-Programm, der Browser oder das Betriebssystem nicht auf dem aktuellen Stand sind. Ähnlich verhält es sich bei der Kommunikation über VPN.

**10. Welche der folgenden Informationen hilft Dir bei der Entscheidung, ob eine Shopping-Website vertrauenswürdig ist?**

a) Die Adresse der Website fängt mit „https://“ an.
b) Ein Gütestempel auf der Website sagt: „100% sicher“.
c) Recherchiere und sammle Informationen zur Website und deren Vertrauenswürdigkeit.
d) Lies auf der Website und schaue Dir die positiven Kommentare der Nutzer dort an.

Richtige Antwort: c)

Begründung: Bösartige Websites können auch über „https“ laufen und Sicherheitssiegel können leicht gefälscht werden. Der Website-Eigentümer kann auch gefälschte Bewertungen anderer Kunden auf seine Website stellen. Am besten ist es, ein wenig zu recherchieren, um zu sehen, ob die Website einen guten Ruf hat. Der Ruf und die Glaubwürdigkeit der Website spielen beim Online-Einkauf eine wichtige Rolle.

**11. Was wird bei Angriffen mit Hilfe von Homoglyphen oder Homografen verwendet?**

a) Angreifer missbraucht die Ähnlichkeiten von Schriftzeichen.
b) Angreifer sendet einen infizierten Anhang.
c) Angreifer sendet eine Phishing-E-Mail an die gesamte Belegschaft.
d) Keine der oben aufgeführten Methoden.

**Richtige Antwort: a)**

Begründung: Angreifer nutzen diese Taktiken, um Benutzer zu verwirren. Sie werden als Homoglyphen bezeichnet. Ein Homoglyphen-Angriff basiert darauf, einen Buchstaben in einer URL durch einen anderen zu ersetzen, der sehr ähnlich oder sogar identisch aussieht, aber zu einem anderen Alphabet gehört. Das menschliche Auge erkennt den Unterschied nicht, aber ein Computer verarbeitet jedes Zeichen unter einem anderen Code.

**12. Welche Art des Umgangs mit einem Passwort ist sicher?**

a) Weitergabe des Passworts auf Anfrage des Vorgesetzten.
b) Aufbewahren des Passworts in Papierform, in einem Umschlag, in einer abgeschlossenen Schreibtischschublade.
c) Weitergabe des Passworts auf Anfrage des IT (Security) Teams.
d) Das Passwort auf die Rückseite der Tastatur kleben.

**Richtige Antwort: b)**

Begründung: Ein mit anderen Personen geteiltes Passwort ist trotz Länge oder anderen Komplexitäten nicht sicher.

**13. Welche Aussage über die Benutzung von Passwörtern im beruflichen Einsatz trifft zu?**

a) Es gibt keine Beschränkungen.
b) Passwörter sollten komplex sein. Es ist erlaubt, die Firmenpasswörter auch außerhalb der Firma zu nutzen.
c) Passwörter sollten von komplex sein. Es ist verboten, die Firmenpasswörter auch außerhalb der Firma zu nutzen.
d) Passwörter sollten komplex sein. Es ist erlaubt, sie mit Kollegen zu teilen.

**Richtige Antwort: c)**

Begründung: Die Mitarbeitenden sind dazu verpflichtet, Passwörter in hoher Komplexität zu wählen, d. h. ausreichend lang und nicht leicht erratbar.

Wie Du ein sicheres Passwort erstellst:

Denke Dir einen leicht merkbaren, aber abstrakten Satz aus. „Ich bestelle gern mindestens fünf Zwiebelrollmopse mit einem Bier und saurer Milch."

Ersetze die Wörter im Satz durch Zahlen und Sonder-, Leer- und Satzzeichen. „Ich bestelle gern mindestens fünf Zwiebelrollmopse mit einem Bier und saurer Milch." zu „Ich bestelle gern > 5 Zwiebelrollmopse, 1 Bier + saure Milch!". Dies ergibt eine komplexe Passphrase, die von möglichen Angreifern schwer zu knacken ist.

Die Zusammensetzung des Passworts, bzw. den Satz/die Phrase selbst solltest NUR DU kennen.

Das Passwort, das für den Zugang zu Informationssystemen (IS) innerhalb der Firma genutzt wird, darf nicht für private Zugänge verwendet werden.

Verrate Dein Passwort NIEMANDEM! Auch nicht Deinen Kollegen, auch nicht Deiner Familie, Deinem Chef oder dem IT Support - auch dann nicht, wenn Du im Urlaub bist und „dringend" eine Datei aus dem System brauchst. Für das Lösen von solchen Situationen ist der IT Support zuständig.

**14. Du empfängst einen Anruf. Der Anrufer erfragt vertrauliche Informationen. Wie reagierst du?**

a) Bitte den Anrufer diese Anfrage per signierter E-Mail von seinem Firmen-E-Mail-Account zu senden und verifiziere die Identität des Anrufers.
b) Bestehe darauf, die Person auf ihrem Telefon zurückzurufen.
c) Frage nach dem Namen seines Vorgesetzten bevor Du seiner Nachfrage nachkommst.
d) Komme der Nachfrage sofort nach, da der Anrufer ja jetzt im Home-Office arbeitet und nicht an sein Firmen(festnetz)telefon herankommt.

**Richtige Antwort: a)**

Begründung: Vishing ist ein Versuch, durch Social Engineering am Telefon persönliche oder sensible Informationen zu entlocken oder den Benutzer zu bestimmten Aktionen zu bringen - z.B. eine Fernverwaltungssoftware zu installieren und den Computer von einem „Techniker" reparieren zu lassen.
Du solltest den Anrufer bitten, jede Anfrage nach sensiblen Informationen über eine signierte E-Mail von der Firmenadresse aus zu senden, und vor der Antwort solltest Du die Identität des Anrufers überprüfen. Wenn die Person eine Rückrufnummer oder die Nummer seines Managers angibt, kann dies Teil des Betrugs sein - verwende diese also nicht. Suche stattdessen nach der offiziellen Telefonnummer des Unternehmens und rufe die betroffene Organisation an.

**15. Was ist der beste Weg die Vertraulichkeit von Daten auf einem Notebook zu schützen, wenn dieses gestohlen wurde?**

a) Full Disk Encryption (Verschlüsselung der gesamten Festplatte)
b) Anti-Theft (Ortung von Geräten per GPS)
c) Antivirus-Software
d) Backup

**Richtige Antwort: a)**

Begründung: Der beste Weg, Firmendaten auf dem gestohlenen Notebook zu schützen, ist die vollständige Verschlüsselung der gesamten Festplatte. Anti-Theft kann evtl. das Notebook orten, jedoch ist durch den Dieb eine unverschlüsselte Festplatte immer noch auslesbar. Anti-Malware/Virus ist im beschriebenen Fall nutzlos, da die Programme nicht den Zugriff auf vertrauliche Daten verhindern. Ein Backup kann die Verfügbarkeit der Daten garantieren, jedoch nicht die Vertraulichkeit dieser.

**16. Dürfen interne oder vertrauliche Firmeninformationen in nicht-autorisierten Clouds gespeichert und bearbeitet werden? (Google Docs, Google Translate, Google Drive; Dropbox)**

a) Ja
b) Nein

**Richtige Antwort: b)**

Begründung: Interne oder vertrauliche Firmeninformationen dürfen nur bei genehmigten Cloud-Dienstleistern, die in der „Liste der autorisierten Cloud Dienstleistungen" (*bitte fügen Sie einen Verweis auf Ihre Liste der autorisierten Cloud Dienstleistungen ein*) genannt sind, gespeichert und bearbeitet werden. Informationen aus der Kategorie VERTRAULICH oder STRENG VERTRAULICH dürfen auch bei autorisierten Cloud-Dienstleistern NICHT gespeichert oder bearbeitet werden.

**17. Welche Informationen solltest Du auf Deinen privaten Social Media Profilen nicht veröffentlichen? (Mehrfachauswahl möglich)**

a) Informationen über die internen Abläufe der Firma.
b) Firmen-E-Mails und andere Kontaktinformationen.
c) Lustige Geschichten, die Du im Urlaub erlebt hast.
d) Deine persönlichen Daten, wie Deine Adresse oder Dein Geburtsdatum.

**Richtige Antwort: a), b), d)**

Begründung: Informationen über die internen Abläufe der Firma, Firmen-E-Mails und andere Kontaktinformationen, sowie Deine persönlichen Daten haben den Charakter vertraulicher Informationen. Sie sollten daher nirgends veröffentlicht werden.

**18. Warum ist es wichtig Deinen Bildschirm zu sperren, wenn Du gerade nicht an Deinem Computer arbeitest?**

a) Um die automatische Installation von Schadcode zu vermeiden.
b) Um zu verhindern, dass eine nicht autorisierte Person Deine Zugangsberechtigungen für den Zugang zu firmeninternen Daten missbrauchen kann.
c) Um eine fehlerfreie Sicherung Deiner Daten zu gewährleisten.
d) Um das Urheberrecht einzuhalten.

Richtige Antwort: b)

Begründung: Eine unautorisierte Person hat im Fall, dass ein Computer nicht gesperrt ist (d.h. es wird kein Anmeldepasswort zum Fortsetzen der Arbeit verlangt) Kontrolle über das Gerät. Diese Person verfügt somit über alle Zugriffsrechte, über die auch der betroffene User verfügt. Das heißt, dass sie Zugang zu allen firmeninternen Daten hat, auf die auch der Mitarbeitende Zugriff hat.

**19. Wähle aus, welche der folgenden Möglichkeiten NICHT zur Sicherheit beiträgt.**

a) Die Mitarbeitenden sind verpflichtet, ihr Notebook bei einer Unterbrechung der Arbeit zu sperren.
b) Die Mitarbeitenden sind verpflichtet, das „Clear-Desk-" und „Clear-Screen-Prinzip" einzuhalten.
c) Die Mitarbeitenden sind verpflichtet, Wartungen und Reparaturen an Dienstgeräten selbst vorzunehmen.
d) Die Mitarbeitenden dürfen sich vertrauliche Informationen nicht in Räumen ansehen, in denen diese ebenfalls von nicht autorisierten Personen gesehen werden können.

Richtige Antwort: c)

Begründung: Die Grundsätze der physischen Sicherheit erfordern bei einer Unterbrechung der Arbeit das Sperren des Arbeitsgerätes. Weiterhin müssen die Prinzipien des „Clear-Desk" und „Clear-Screen" angewandt werden. Außerdem dürfen vertrauliche Informationen nicht in Räumen angesehen werden, in denen diese auch von nicht autorisierten Personen gesehen werden könnten. Jedoch dürfen Wartungen und Reparaturen von Arbeitsgeräten AUSSCHLIESSLICH von autorisiertem Servicepersonal durchgeführt werden.

ESET ist ein europäisches Unternehmen mit Hauptsitz in Bratislava (Slowakei). Seit 1987 entwickelt ESET preisgekrönte Sicherheits-Software, die bereits über 110 Millionen Benutzern hilft, sichere Technologien zu genießen. Das breite Portfolio an Sicherheitsprodukten deckt alle gängigen Plattformen ab und bietet Unternehmen und Verbrauchern weltweit die perfekte Balance zwischen Leistung und proaktivem Schutz. Das Unternehmen verfügt über ein globales Vertriebsnetz in über 200 Ländern und Niederlassungen u.a. in Jena, San Diego, Singapur und Buenos Aires. Für weitere Informationen besuchen Sie www.eset.de oder folgen uns auf LinkedIn, Facebook und Twitter.

© 1992 - 2021 ESET, spol. s r.o. - All rights reserved. Trademarks used therein are trademarks or registered trademarks of ESET, spol. s r.o. or ESET North America. All other names and brands are registered trademarks of their respective companies.

ESET.DE | ESET.AT | ESET.CH