Co-funded by the Erasmus+ Programme of the European Union

InCyT-Trainingsmodule

Informationssicherheit für Manager Einheit -2 Woche-3 Bezeichnung des Referats: Management der Informationssicherheit -1	
Lernaktivitäten	❑ **Webinar** ❑ **Übungen** ❑ **Workshop** ❑ **Präsentation** ❑ **Sonstiges** Streaming-Webinar, Text, Übungen zur Selbsteinschätzung, Übungen mit Antworten in Diskussionsforen und Diskussion mit Trainer/Mentor
Verantwortliche Lehrende	• Fatma Gökdemir • Ali Gökdemir
Ziele der Lernaktivitäten	1. Informationssicherheit 2. Richtlinien zur Informationssicherheit 3. Rollen in der Informationssicherheit
Zu erwerbende Fertigkeiten	• IS 1 • IS 3 • MS 3
Dauer der Lernaktivität	2 Wochen
Lernanforderungen	***Was wird benötigt?*** • Mittlere Computerkenntniss

Co-funded by the
Erasmus+ Programme
of the European Union

Kurzinformationen zum Modul

Beschreibung
Die Informationssicherheit ist von großer Bedeutung für die Kontinuität jeder Organisation und gewährleistet den Schutz der kritischen Informationen und anderer Informationswerte der Organisation in verschiedenen Umgebungen, insbesondere in elektronischen Umgebungen. Nicht nur große Unternehmen und Holdings, sondern auch KMU, Regierungsbehörden, gemeinnützige Organisationen, Schulen oder Einzelpersonen sind ständig mit Problemen und Risiken der Informationssicherheit konfrontiert, wenn auch auf unterschiedlichem Niveau. Bei Investitionen zur Bewältigung dieser Risiken ist die teuerste und komplexeste Lösung nicht immer die sicherste Lösung. Jede Person oder Organisation muss die am besten geeignete und richtige Lösung wählen und umsetzen. Es sollte nicht vergessen werden, dass eine einfache und kostengünstige Sicherheitslösung für manche Einrichtungen unzureichend sein kann, während dieselbe Lösung für eine andere Einrichtung ausreichend und wirksam sein kann. Die Informationssicherheit ist jedoch keine Arbeit, die man anfängt und dann beendet. Das Management der Informationssicherheit ist ein Lebenszyklus, der ständig verwaltet und geprüft werden muss, solange es Einrichtungen und Informationen gibt. In diesem Modul werden das Konzept der Informationssicherheit, seine Bedeutung und die Maßnahmen zur Informationssicherheit erläutert. Das Thema wurde durch ein praktisches Beispiel unterstützt

Inhalt des Lernmaterials

1. Informationssicherheit

Bei der Informationssicherheit geht es darum, den unbefugten oder unerlaubten Zugriff auf Informationen sowie deren Nutzung, Änderung, Weitergabe, Zerstörung, Austausch und Beschädigung zu verhindern. Sie besteht aus drei grundlegenden Elementen: Vertraulichkeit, Integrität und Zugänglichkeit (Abbildung 1). Wenn eines dieser drei grundlegenden Sicherheitselemente beschädigt wird, entsteht eine Sicherheitslücke.

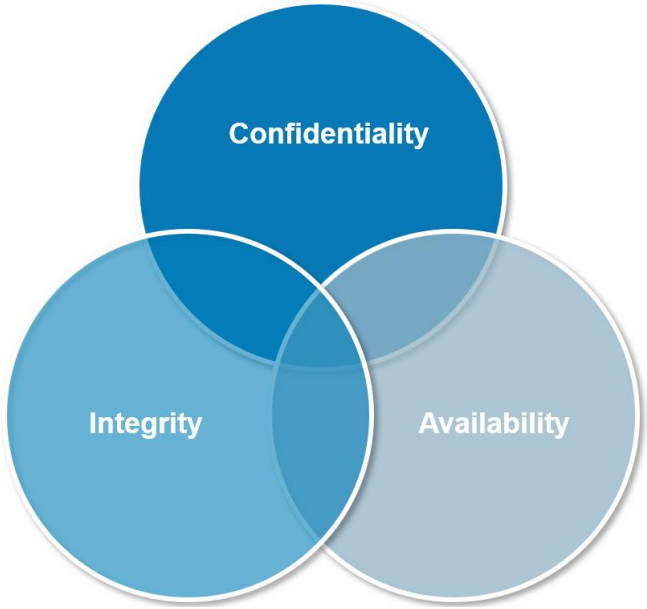


Abbildung 1. Elemente der Informationssicherheit

- Vertraulichkeit: Sie ist der Schutz von Informationen vor unbefugtem Zugriff und unbefugter Kenntnisnahme.
- Integrität: Informationen werden nicht von Unbefugten verändert.
- Zugänglichkeit: Die Informationen sind für befugte Personen bei Bedarf zugänglich und nutzbar.

1.1. Was ist eine Informationssicherheitspolitik?

Die Sicherheitsbedrohungen entwickeln sich ständig weiter, und die Anforderungen an die Einhaltung von Vorschriften werden immer komplexer. Unternehmen müssen eine umfassende Informationssicherheitsrichtlinie erstellen, um beiden Herausforderungen gerecht zu werden.

Eine Informationssicherheitspolitik (ISP) ist eine Reihe von Regeln, Richtlinien und Verfahren, die sicherstellen sollen, dass alle Endbenutzer und Netzwerke innerhalb einer Organisation die Mindestanforderungen an die IT-Sicherheit und den Datenschutz erfüllen. Eine Informationssicherheitspolitik ermöglicht es, ein Sicherheitsprogramm zu koordinieren und durchzusetzen und Sicherheitsmaßnahmen an Dritte und externe Prüfer zu kommunizieren.

1.2. Was ist der Zweck einer Informationssicherheitspolitik?

Eine Informationssicherheitspolitik zielt darauf ab, Schutzmaßnahmen zu ergreifen und die Verbreitung von Daten auf die Personen zu beschränken, die dazu berechtigt sind. Organisationen schaffen ISPs, um:

- Festlegung eines allgemeinen Konzepts für die Informationssicherheit
- Dokumentieren Sie Sicherheitsmaßnahmen und Richtlinien für die Zugangskontrolle von Benutzern
- Erkennen und Minimieren der Auswirkungen gefährdeter Informationsbestände, wie z. B. des Missbrauchs von Daten, Netzwerken, mobilen Geräten, Computern und Anwendungen
- den Ruf der Organisation zu schützen
- Einhaltung rechtlicher und regulatorischer Anforderungen wie ENISA, NIST, GDPR, HIPAA und FERPA
- die Daten ihrer Kunden, wie z. B. Kreditkartennummern, zu schützen
- Bereitstellung wirksamer Mechanismen zur Beantwortung von Beschwerden und Anfragen im Zusammenhang mit tatsächlichen oder vermeintlichen Cybersicherheitsrisiken wie Phishing, Malware und Ransomware
- Beschränkung des Zugangs zu wichtigen Informationstechnologien auf Personen, die über eine akzeptable Nutzung verfügen

1.3. Warum ist eine Informationssicherheitspolitik wichtig?

Die Erstellung einer wirksamen Informationssicherheitsrichtlinie, die alle Compliance-Anforderungen erfüllt, ist ein wichtiger Schritt zur Vermeidung von Sicherheitsvorfällen wie Datenlecks und Datenschutzverletzungen.

ISPs sind für neue und etablierte Unternehmen wichtig. Die zunehmende Digitalisierung bedeutet, dass jeder Mitarbeiter Daten erzeugt und ein Teil dieser Daten vor unbefugtem Zugriff geschützt werden muss. Je nach Branche können sie sogar durch Gesetze und Vorschriften geschützt sein.

Sensible Daten, persönlich identifizierbare Informationen (PII) und geistiges Eigentum müssen nach einem höheren Standard geschützt werden als andere Daten.

Ob Sie es wollen oder nicht, Informationssicherheit (InfoSec) ist auf jeder Ebene Ihres Unternehmens wichtig. Und außerhalb Ihrer Organisation.

Informationssicherheitsrichtlinien können für eine Organisation folgende Vorteile haben:

- **Erleichtert die Datenintegrität, -verfügbarkeit und -vertraulichkeit: Wirksame** Informationssicherheitsrichtlinien standardisieren Regeln und Prozesse, die vor Vektoren schützen, die die Datenintegrität, -verfügbarkeit und -vertraulichkeit gefährden.
- **Schutz sensibler Daten -** Informationssicherheitsrichtlinien haben den Schutz von geistigem Eigentum und sensiblen Daten, wie z. B. personenbezogene Daten (PII), zur Priorität.
- **Minimierung des Risikos von Sicherheitsvorfällen -** Eine Informationssicherheitsrichtlinie hilft Unternehmen bei der Festlegung von Verfahren zur Identifizierung und Eindämmung von Schwachstellen und Risiken. Sie enthält auch Details zu schnellen Reaktionen, um den Schaden bei einem Sicherheitsvorfall zu minimieren.
- **Führt Sicherheitsprogramme im gesamten Unternehmen aus -** Informationssicherheitsrichtlinien bilden den Rahmen für die Umsetzung von Verfahren.
- **Bietet eine klare Sicherheitserklärung für Dritte** - Informationssicherheitsrichtlinien fassen die Sicherheitslage des Unternehmens zusammen und erläutern, wie das Unternehmen IT-Ressourcen und -Anlagen schützt. Sie erleichtern die schnelle Reaktion auf Informationsanfragen von Kunden, Partnern und Wirtschaftsprüfern.
- **Unterstützung bei der Einhaltung gesetzlicher Vorschriften** - Die Erstellung einer Informationssicherheitsrichtlinie kann Unternehmen dabei helfen, Sicherheitslücken in Bezug auf gesetzliche Vorschriften zu erkennen und zu schließen.

1.4. Was sollte in einer Informationssicherheitspolitik enthalten sein?

Es kann schwierig sein, eine Informationssicherheitspolitik von Grund auf zu entwickeln; sie muss robust sein und Ihr Unternehmen in jeder Hinsicht schützen. Sie sollte sämtliche Software, Hardware, physische Parameter, Humanressourcen, Informationen und Zugangskontrollen abdecken. Außerdem muss sie flexibel sein und Raum für Überarbeitungen und Aktualisierungen bieten, und vor allem muss sie praktisch und durchsetzbar sein. Wunschdenken hilft Ihnen nicht

weiter, wenn Sie eine Informationssicherheitspolitik entwickeln. Sie müssen mit den wichtigsten Interessengruppen zusammenarbeiten, um eine Richtlinie zu entwickeln, die für Ihr Unternehmen und die Mitarbeiter, die für die Umsetzung der Richtlinie verantwortlich sein werden, geeignet ist.

1. ***Richtlinie zur akzeptablen Nutzung***

Diese Richtlinie regelt die zulässige Nutzung von Computern und des Internets in Ihrem Unternehmen. Die unsachgemäße Nutzung des Internets oder von Computern birgt für Ihr Unternehmen Risiken wie Virenangriffe, gefährdete Netzwerksysteme und -dienste sowie rechtliche Probleme. Daher ist es wichtig, schriftlich festzuhalten, welche Nutzung zulässig ist und welche nicht.

In einer Richtlinie zur akzeptablen Nutzung sollte dargelegt werden, wie die Mitarbeiter die Geräte des Unternehmens schützen müssen, z. B. indem sie ihre Computer abschließen, wenn sie sich nicht an ihrem Arbeitsplatz befinden, oder indem sie Tablets oder andere elektronische Geräte, die sensible Informationen enthalten könnten, schützen. Sie sollte auch darlegen, welche Rechte das Unternehmen hat und welche Aktivitäten auf den Geräten und im Netzwerk des Unternehmens nicht verboten sind.

2. ***Politik der sauberen Schreibtische***

Eine "Clean Desk"-Richtlinie konzentriert sich auf den Schutz von Sachwerten und Informationen. Im Idealfall wird mit dieser Richtlinie sichergestellt, dass alle sensiblen und vertraulichen Materialien weggeschlossen oder anderweitig gesichert werden, wenn sie nicht gebraucht werden oder ein Mitarbeiter seinen Arbeitsplatz verlässt. Diese Richtlinie sollte die Mindestanforderungen für die Aufrechterhaltung eines sauberen Schreibtisches festlegen, z. B. wo vertrauliche Informationen über Mitarbeiter, geistiges Eigentum, Kunden und Lieferanten aufbewahrt und abgerufen werden können. Sie sollte auch regeln, welche Arten von Materialien geschreddert oder weggeworfen werden müssen, ob Passwörter verwendet werden müssen, um Dokumente von einem Drucker abzurufen, und welche Informationen oder Gegenstände mit einem physischen Schloss gesichert werden müssen. Eine "Clean Desk"-Richtlinie ist nicht nur ein allgemeiner und wichtiger Bestandteil jeder Informationssicherheitsrichtlinie, sondern entspricht auch der Norm ISO 27001/17799 und wird Ihrem Unternehmen helfen, ein Zertifizierungsaudit zu bestehen.

3. ***Richtlinie zur Reaktion auf Datenverletzungen***

Dies wird auch als Plan zur Reaktion auf einen Vorfall bezeichnet. Der Zweck einer Richtlinie zur Reaktion auf Datenschutzverletzungen besteht darin, die Ziele und die Vision dafür festzulegen, wie Ihr Unternehmen auf eine Datenschutzverletzung reagieren wird. Dieser Plan trägt dazu bei, das Risiko, Opfer eines Cyberangriffs zu werden, zu mindern, da er detailliert beschreibt, wie Ihr

Unternehmen die Datenbestände während des gesamten Reaktionsprozesses auf einen Vorfall schützen will.

In dieser Richtlinie sollte festgelegt werden, für wen sie gilt und wann sie in Kraft tritt, einschließlich der Definition eines Verstoßes, der Aufgaben und Zuständigkeiten der Mitarbeiter, der Standards und Messgrößen, der Berichterstattung, der Abhilfemaßnahmen und der Feedback-Mechanismen.

4. Disaster Recovery Plan Richtlinie

Diese Richtlinie unterscheidet sich von einem Reaktionsplan für Datenverletzungen, da es sich um einen allgemeinen Notfallplan handelt, der regelt, was im Falle einer Katastrophe oder eines Ereignisses zu tun ist, das eine längere Verzögerung des Dienstes verursacht. Diese Richtlinie sollte das Verfahren zur Wiederherstellung von Systemen, Anwendungen und Daten während oder nach einer Katastrophe, die einen größeren Ausfall verursacht, beschreiben. Dieser Wiederherstellungsplan sollte jährlich aktualisiert werden.

Der Notfallplan sollte diese Elemente abdecken:

- Notfallplan für die Kontaktaufnahme. Führen Sie explizit auf, wer kontaktiert werden muss, wann sie kontaktiert werden müssen und wie Sie sie kontaktieren werden.
- Nachfolgeplan. Beschreiben Sie die Zuständigkeiten für den Fall, dass normales Personal nicht verfügbar ist, um seine Aufgaben zu erfüllen.
- Plan zur Datenklassifizierung. Detaillierte Angaben zu den auf allen Systemen gespeicherten Daten, ihrer Kritikalität und ihrer Vertraulichkeit.
- Liste der Wichtigkeit der Dienste. Führen Sie alle erbrachten Leistungen in der Reihenfolge ihrer Wichtigkeit auf.
- Plan zur Datensicherung und -wiederherstellung. Geben Sie an, welche Daten wo und wie oft gesichert werden. Erläutern Sie auch, wie die Daten wiederhergestellt werden können.
- Plan für den Austausch von Ausrüstung. Beschreiben Sie, welche Infrastrukturdienste für die Wiederaufnahme der Dienste für die Kunden erforderlich sind.
- Öffentliche Kommunikation. Legen Sie fest, wer für die externe PR-Funktion zuständig ist, und geben Sie Richtlinien vor, welche Informationen weitergegeben werden können und sollen.
- Es ist wichtig, dass sich das Managementteam Zeit nimmt, um den Notfallwiederherstellungsplan zu testen. Bei diesen Tests, die auch als Tabletop-Übungen bezeichnet werden, geht es darum, Probleme zu erkennen, die in der Planungsphase nicht offensichtlich sind und zum Scheitern des Plans führen könnten. Auf diese Weise kann das Team den Plan anpassen, bevor es zu einer Katastrophe kommt.

5. *E-Mail-Politik*

E-Mail ist ein wichtiger Kommunikationskanal für Unternehmen aller Art, und der Missbrauch von E-Mails kann die Sicherheit Ihres Unternehmens in vielerlei Hinsicht gefährden, sei es, dass Mitarbeiter vertrauliche Informationen per E-Mail verbreiten oder Ihr Netzwerk versehentlich einem Virus ausgesetzt wird. Es ist wichtig, dass alle Mitarbeiter, Auftragnehmer und Vertreter, die im Namen Ihres Unternehmens tätig sind, den angemessenen Umgang mit E-Mails verstehen und Richtlinien und Verfahren für die Archivierung, Kennzeichnung und Überprüfung von E-Mails festgelegt haben, wenn dies erforderlich ist.

Diese Richtlinie muss die angemessene Verwendung von Firmen-E-Mail-Adressen umreißen und Dinge wie die verbotenen Kommunikationsarten, Datensicherheitsstandards für Anhänge, Regeln für die Aufbewahrung von E-Mails und die Frage, ob das Unternehmen E-Mails überwacht, abdecken. Diese Richtlinie sollte auch für Ihre Mitarbeiter klar formuliert sein, damit sie wissen, welche Verantwortung sie bei der Nutzung ihrer E-Mail-Adressen tragen und welche Verantwortung das Unternehmen hat, um sicherzustellen, dass E-Mails ordnungsgemäß genutzt werden. Bei dieser E-Mail-Richtlinie geht es nicht darum, eine "Gotcha"-Richtlinie zu erstellen, um Mitarbeiter bei der missbräuchlichen Nutzung ihrer E-Mails zu erwischen, sondern um eine Situation zu vermeiden, in der Mitarbeiter eine E-Mail missbrauchen, weil sie nicht wissen, was erlaubt ist und was nicht.

6. *Richtlinie zum Schutz von Endbenutzer-Verschlüsselungsschlüsseln*

Bestimmte Dokumente und Mitteilungen, die innerhalb Ihres Unternehmens oder an Ihre Endbenutzer verteilt werden, müssen aus Sicherheitsgründen möglicherweise verschlüsselt werden. Legen Sie eine Richtlinie zum Schutz dieser Verschlüsselungsschlüssel fest, damit sie nicht weitergegeben oder in betrügerischer Absicht verwendet werden.

Diese Richtlinie sollte alle Anforderungen an den Schutz von Verschlüsselungsschlüsseln umreißen und die spezifischen betrieblichen und technischen Kontrollen auflisten, die zu ihrer Sicherheit durchgeführt werden. Dazu gehören Dinge wie manipulationssichere Hardware, Sicherungsverfahren und was zu tun ist, wenn ein Verschlüsselungsschlüssel verloren geht, gestohlen oder in betrügerischer Absicht verwendet wird.

7. *Richtlinie zum Passwortschutz*

Ihre Mitarbeiter haben wahrscheinlich eine Vielzahl von Passwörtern, die sie im Auge behalten und tagtäglich verwenden müssen, und Ihr Unternehmen sollte klare, eindeutige Standards für die Erstellung sicherer Passwörter für ihre Computer, E-Mail-Konten, elektronischen Geräte und jeden Punkt, an dem sie Zugang zu Ihren Daten oder Ihrem Netzwerk haben, festlegen.

In dieser Richtlinie muss auch festgelegt werden, was die Mitarbeiter mit ihren Passwörtern tun dürfen und was nicht. Es mag offensichtlich erscheinen, dass sie ihre Passwörter nicht in eine E-Mail schreiben oder sie an Kollegen weitergeben sollten, aber Sie sollten nicht davon ausgehen, dass dies allen bekannt ist. Geben Sie Ihren Mitarbeitern alle Informationen, die sie benötigen, um sichere Passwörter zu erstellen und sie sicher aufzubewahren, um das Risiko von Datenschutzverletzungen zu minimieren.

Schließlich sollte diese Richtlinie darlegen, was Ihre Entwickler und IT-Mitarbeiter tun müssen, um sicherzustellen, dass alle von Ihrem Unternehmen betriebenen Anwendungen oder Websites Sicherheitsvorkehrungen treffen, um die Passwörter der Benutzer zu schützen.

Untersuchungen, die in den letzten zehn Jahren weltweit durchgeführt wurden, zeigen, dass die bevorzugten Passwörter der Benutzer folgende sind:

- 123456
- Passwort
- qwerty
- 111111
- 123123
- 987654321
- 123456789
- asdfgh

Trotz jährlicher Warnungen hat sich an dieser Liste nicht viel geändert. Daher wird den Benutzern empfohlen, eine Reihe von Regeln für die Festlegung von Kennwörtern zu befolgen. Diese Regeln sind im Folgenden aufgeführt:

- Festlegung von Komplexitätsanforderungen, wie z. B. die Erfüllung der Mindestanforderungen an Zeichen
- Keine Auswahl bereits verwendeter Passwörter
- Regelmäßiges und eventuell häufiges Ändern der Passwörter
- Die verwendeten Passwörter sollten nicht wie in der obigen Liste aus gängigen und schwach verwendeten Passwörtern ausgewählt werden

Das National Institute of Standards and Technology (NIST) hat sich zum Ziel gesetzt, das Problem der Passwortpolitik zu lösen, um Passwörter festzulegen und bestimmte Standards zu erreichen. Das NIST legt Details zu Passwörtern fest und wie diese verwaltet und gespeichert werden sollten. Demnach sollten mögliche Passwörter mit einer Liste von häufig verwendeten und bekannten Werten abgeglichen werden. Die Überlegungen zur Festlegung von Passwörtern sind wie folgt:

- Die vom Benutzer eingegebenen Passwörter sollten aus mindestens acht alphanumerischen Zeichen bestehen.

- Es sollte sich nicht um Passwörter handeln, die aus früheren Verstößen stammen.
- Es sollten keine Wörter aus dem Wörterbuch verwendet werden.
- Es sollten keine Daten zwischen 1900-2020 enthalten sein, wie z. B. Geburtsdaten.
- Keine sich wiederholenden oder aufeinanderfolgenden Zeichen (z. B. aaaaaaaa oder 1234abcd)
- Spezifische Wörter für den Verwendungszweck, wie der Name des Dienstes, der Benutzername und davon abgeleitete Begriffe, sollten nicht verwendet werden.

Die oben genannten Kriterien sollten bei der Festlegung von Passwörtern berücksichtigt werden, und es sollten Passwörter mit komplexen Strukturen erstellt werden.

Passwortkomplexität: Passwortkomplexität ist definiert als die Anzahl der Passwörter, die stark sind, d.h. ein Passwort muss eine Reihe von Regeln erfüllen. Der Schlüssel zur Passwortkomplexität Die Regeln lauten wie folgt:

- Das Passwort darf nicht den Kontonamen oder Variationen des Kontonamens enthalten.
- Das Passwort muss sowohl Großbuchstaben (A-Z) als auch Kleinbuchstaben (a-z) enthalten.
- Sonderzeichen **(~! @ # $% ^ & * _- + = `| \ () {} [] :;" '<>,.? /)** (Dies sind die Zeichen, die normalerweise mit der ALT-Taste erscheinen. Währungen wie z. B. Euro-Symbole gelten jedoch nicht als Sonderzeichen).
- Die Mindestanzahl der Zeichen muss beachtet werden. Dieser Wert ist von System zu System und von Benutzer zu Benutzer unterschiedlich. kann sich ändern.

Die Mindestlänge des Passworts sollte 8 Zeichen betragen, empfohlen werden 12 Zeichen.
Wenn Passwörter mit mindestens 8 Zeichen nach den oben genannten Regeln erstellt werden, bedeutet dies mindestens 218.340.105.584.896 verschiedene Möglichkeiten für ein einziges Passwort. Die Wahrscheinlichkeit des generierten Passworts macht einen Brute-Force-Angriff sehr schwierig, aber das Passwort ist immer noch nicht unmöglich zu knacken. Um ein nahezu unmöglich zu knackendes Passwort zu erhalten, muss die Anzahl der Zeichen erhöht werden. Je höher die Mindestanzahl der Zeichen ist, desto länger dauert es, das Kennwort zu knacken.
Neben den Vorteilen der Passwortkomplexität bringt sie auch einige Herausforderungen mit sich. Eine der wichtigsten ist das Vergessen des Passworts. Es ist schwierig, sich ein Passwort zu merken, das länger ist und Sonderzeichen enthält. Vor allem, wenn alle Passwörter unterschiedlich sind, ist es schwierig, sie sich zu merken und sie nicht mit anderen zu verwechseln. Daher sollte bei der Erstellung von Passwörtern eine gewisse Logik beachtet werden.

Zum Beispiel;

- Ich bin das 2. Kind in einer Familie mit 3 Kindern!

Sie können einen Satz wie diesen aus Ihrem eigenen Leben schreiben. Wenn Sie die ersten Buchstaben und Sonderzeichen des Satzes nehmen, erhalten Sie ein Passwort wie **Ibd2KieFm3K!**

- Ich bin am 19. Juli Mitglied dieser Website (über Bildung) geworden.

Sie können einen Satz wie "Ich bin am 19. Juli Mitglied dieser Website (über Bildung) geworden (englisch)" entsprechend dem Interessengebiet der Website und dem Datum der Mitgliedschaft anpassen, damit Sie es nicht vergessen. Wenn Sie ihr erstes Zeichen und Sonderzeichen erhalten Sie erhalten dann ein Passwort wie **Iba19JMdW(üB)g.**

8. Richtlinie zum Sicherheitsaktionsplan

Ein Sicherheitsreaktionsplan legt fest, was jedes Team oder jede Geschäftseinheit im Falle eines Sicherheitsvorfalls, wie z. B. einer Datenpanne, zu tun hat. Dem SANS Institute zufolge sollte er "eine Produktbeschreibung, Kontaktinformationen, Eskalationspfade, erwartete Service Level Agreements (SLA), eine Klassifizierung des Schweregrads und der Auswirkungen sowie Zeitpläne für die Schadensbegrenzung und -behebung" enthalten.

Das Wichtigste an einer Sicherheitsstrategie ist, dass sie den verschiedenen Teams hilft, ihre Bemühungen zu bündeln, damit jeder Sicherheitsvorfall so schnell wie möglich behoben werden kann. Während jede Abteilung ihre eigenen Reaktionspläne haben kann, wird in der Richtlinie für den Sicherheitsreaktionsplan detailliert festgelegt, wie sie sich untereinander abstimmen, um sicherzustellen, dass die Reaktion auf einen Sicherheitsvorfall schnell und gründlich erfolgt.

1.5. Beispiele für Informationssicherheitspolitik

Um einen erfolgreichen Cybersicherheitsplan zu erstellen, müssen 5 Hauptpunkte berücksichtigt werden.

a. ***Identifizieren:*** Die Organisation sollte die Cyber-Sicherheitsrisiken, denen sie ausgesetzt ist, kennen, damit sie Prioritäten bei ihren Bemühungen setzen kann.

b. ***Schützen***: Hier geht es darum, geeignete Sicherheitsvorkehrungen zu treffen, um Datenbestände zu schützen und die Auswirkungen eines potenziellen Cybersicherheitsvorfalls zu begrenzen oder einzudämmen. Dazu gehören die Aufklärung und Befähigung der Mitarbeiter innerhalb des Unternehmens, sich der Risiken bewusst zu sein, die Einführung von Verfahren, die sich auf den Schutz der

Netzwerksicherheit und der Vermögenswerte konzentrieren, und möglicherweise die Nutzung einer Cyber-Haftpflichtversicherung, um ein Unternehmen finanziell zu schützen, falls ein Cyberkrimineller in der Lage ist, die vorhandenen Schutzmaßnahmen zu umgehen.

c. ***Erkennen***: Skizzieren Sie die Aktivitäten, die bei der Entdeckung eines Cyberangriffs helfen und eine rechtzeitige Reaktion auf das Ereignis ermöglichen. Um einen Cyberangriff schnell und effizient diagnostizieren zu können, sollten Unternehmen Protokolle zur Datenklassifizierung, zum Asset Management und zum Risikomanagement einführen, die sie warnen, wenn Daten gefährdet zu sein scheinen.

d. ***Reagieren***: Dokumentieren Sie die angemessenen Maßnahmen, die nach der Entdeckung von Bedrohungen der Cybersicherheit ergriffen werden sollten. Die Reaktion eines Unternehmens sollte eine ordnungsgemäße und gründliche Kommunikation mit Mitarbeitern, Aktionären, Partnern und Kunden sowie bei Bedarf mit Strafverfolgungsbehörden und Rechtsberatern umfassen.

e. ***Wiederherstellen***: Legen Sie fest, wie eine Organisation die durch einen Cyberangriff beeinträchtigten Fähigkeiten oder Dienste wiederherstellen kann.

Nahezu jeder Sicherheitsstandard muss eine Art Reaktionsplan für Zwischenfälle vorsehen, denn selbst die solidesten Informationssicherheitspläne und Compliance-Programme können immer noch einer Datenverletzung zum Opfer fallen.

1.6. Übungen zur Informationssicherheitspolitik

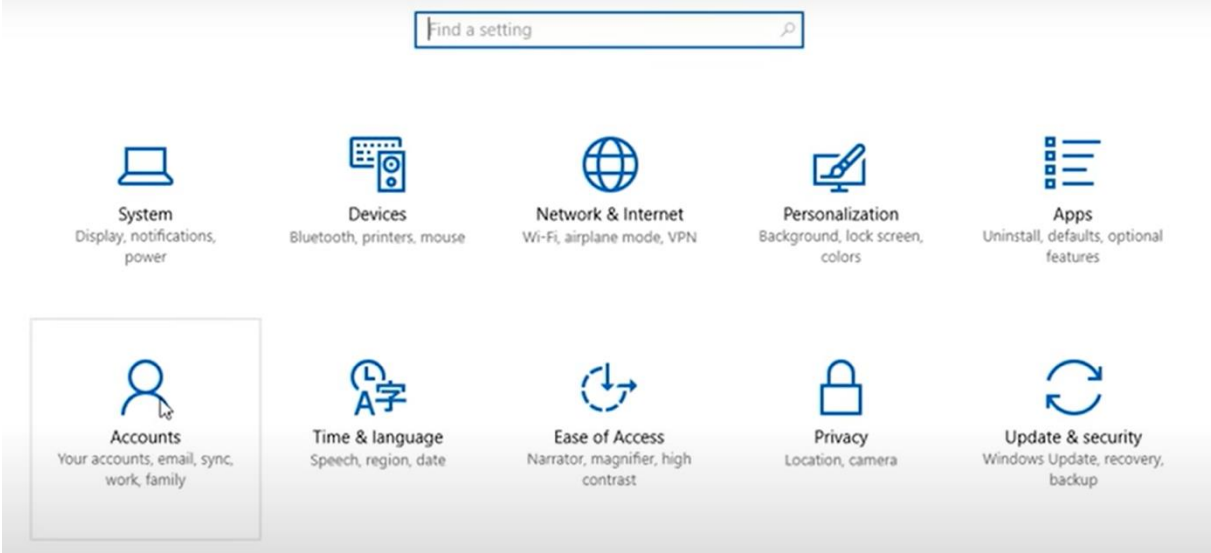
1. Sperren Sie Ihre Sitzung: Verstärken Sie Ihre Online-Konten, indem Sie die stärksten verfügbaren Authentifizierungswerkzeuge aktivieren, z. B. Biometrie (messbare biologische Spuren einer Person), Sicherheitsschlüssel oder einen einmaligen Code, der von einem Anwendungstool auf Ihrem Mobilgerät generiert wird. Ihre Benutzernamen und Passwörter reichen möglicherweise nicht aus, um Konten wie E-Mail, Bankgeschäfte und soziale Medien zu schützen.

Übungen-1:

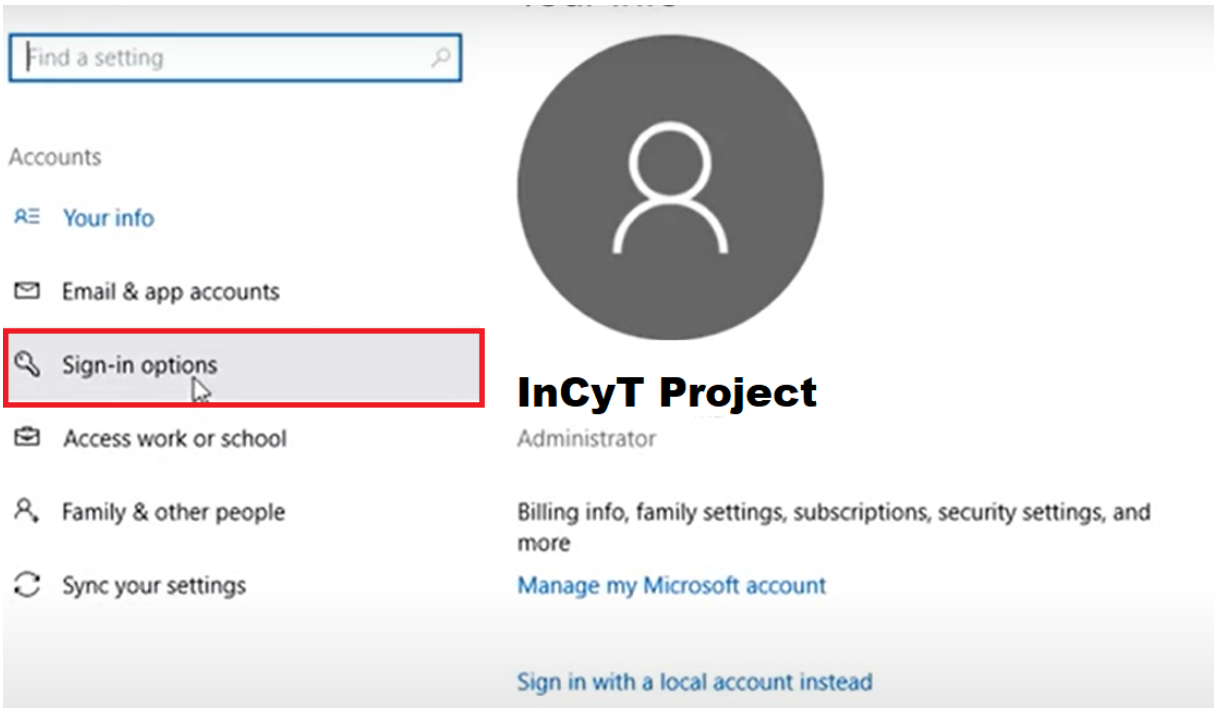
Damit der Computer automatisch gesperrt wird, wenn Sie aufstehen.

Schritt 1: Klicken Sie auf die Schaltfläche Windows-Einstellungen.

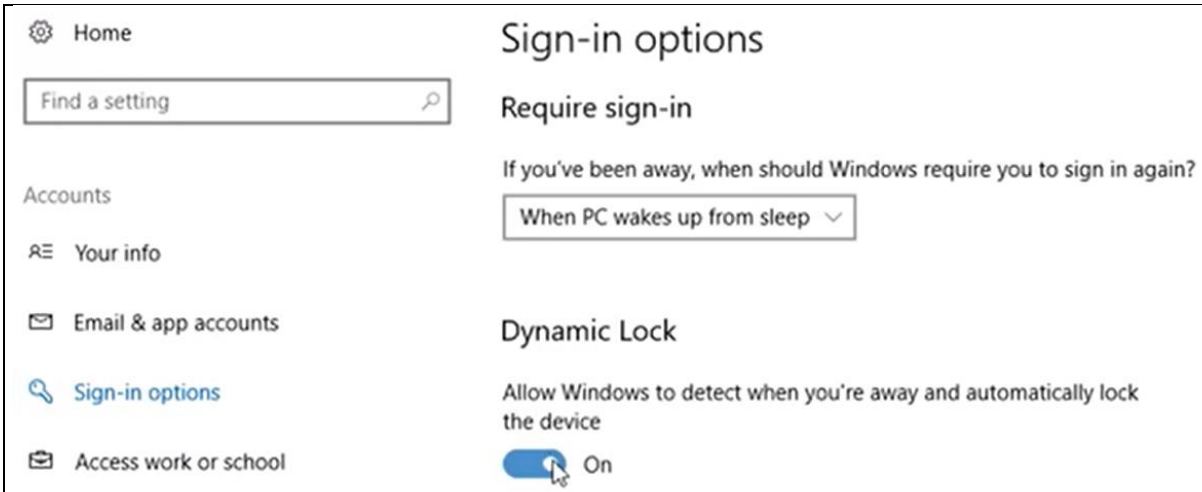
Schritt 2: Klicken Sie auf die Registerkarte Konten.



Schritt 3: Klicken Sie auf den Abschnitt "Anmelden".



Schritt 4: Aktivieren Sie die Spezifikation für die dynamische Sperre.



2- Erstellen Sie ein sicheres Passwort: Das Passwort spielt eine wichtige Rolle bei der Informationssicherheit. Schwache Passwörter können mit Programmen zum Knacken von Passwörtern in kürzester Zeit geknackt werden. Aus diesem Grund ist es notwendig, bei der Erstellung und Verwendung von Passwörtern für alle Geräte und Konten mit größter Sorgfalt vorzugehen und die folgenden Regeln zu beachten. Das Passwort wird im Allgemeinen an vielen Stellen in Computersystemen verwendet. Wir verwenden ein Passwort, wenn wir ein E-Mail-Konto einrichten, ein Passwort für die Anmeldung am Computer festlegen und den Zugriff auf Dateien sperren. Passwörter sollten jedoch nicht schwach oder erratbar sein. Passwörter sollten nach den folgenden Kriterien erstellt werden:

a. Passwörter müssen ***mindestens 8 Zeichen*** lang sein und mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Zahl und ein Sonderzeichen (.-+=_,!@$#*%<>[]{}) enthalten.
b. Das Passwort-Feld ***sollte nicht*** leer gelassen oder voreingestellt ***werden***; ***123456, 01062022, qwerty, password usw.*** Es sollte nicht so festgelegt werden, dass es vorhersehbar und leicht zu knacken ist, wie Wörter, die in jedem Wörterbuch zu finden sind.
c. Passwörter sollten **keine persönlichen Informationen enthalten** (Name Ihres Kindes, Geburtsdatum oder Name der Einrichtung).
d. Für verschiedene Systeme und Konten sollten ***unterschiedliche Passwörter*** erstellt werden.
e. Passwörter sollten häufig ***geändert*** werden (mindestens alle 6 Monate).
f. Passwörter sollten ***nicht*** an Stellen ***aufgeschrieben werden***, die von anderen Personen bemerkt werden können (z. B. neben dem Computer auf Papier), und sie sollten nicht unverschlüsselt im Klartext auf einem Computer oder in einem digitalen Medium gespeichert werden.

g. Kein Bediensteter oder Student sollte sein Passwort (E-Mail-Passwort, Passwort für die elektronische Unterschrift, PC-Passwort usw.) mit einer anderen Person ***teilen***. Die Nutzer sollten wissen, dass sie im Falle einer Weitergabe die volle rechtliche Verantwortung tragen.
h. Eindeutiges Konto, eindeutiges Passwort: Ein eigenes Passwort für jedes Konto hilft, Cyberkriminelle abzuwehren. Trennen Sie zumindest Ihre beruflichen und privaten Konten und stellen Sie sicher, dass Ihre wichtigen Konten die sichersten Passwörter haben.
i. Erinnern Sie sich und bewahren Sie es sicher auf: Starke Passwörter sind schwer zu erstellen und zu merken. Legen Sie Ihre Passwörter so fest, dass sie nur Ihnen etwas sagen und Sie sie sich merken können, oder bewahren Sie sie an einem sicheren Ort und in einem sicheren Format auf. Alternativ können Sie auch einen Dienst wie einen Passwort-Manager nutzen, um Ihre Passwörter zu verwalten.

Übungen-2:

Passwortsicherheit bei der Einrichtung eines E-Mail-Kontos über den E-Mail-Anbieter Ihres Unternehmens oder eine Anwendung oder Website eines öffentlichen E-Mail-Anbieters

Schritt 1: Öffnen Sie die Website oder Anwendung.
Schritt 2: Geben Sie Ihre persönlichen Daten ein, um ein Konto zu erstellen.

Schritt 3: Verwenden Sie beim Erstellen eines Passworts Kombinationen aus Großbuchstaben, Kleinbuchstaben, Ziffern und Symbolen.
Um das Kennwort für den Benutzer leicht zu merken, können Sie es kodieren. Sie können zum Beispiel einen Satz schreiben, der zum Thema passt, und die ersten Buchstaben, Zahlen und Sonderzeichen des Satzes verwenden, den Sie geschrieben haben.

This Cybersecurityproject is supported byErasmus+ **2021**

Schritt 4: Wir legen unser Passwort fest: TcpisbE+2021
Schritt 5: Stellen Sie sicher, dass das Passwort aus mindestens 8 Zeichen besteht. 12 Zeichen sind vorzuziehen. Man kann sagen, dass das von uns verwendete Passwort geeignet ist, weil es 12 Zeichen hat.

3- Zugang zu sicheren Websites (Safe Browser): Wenn Sie online gehen, um einzukaufen oder Nachrichten zu lesen, verwenden Sie einen Browser. Browser sind eine der wichtigsten Möglichkeiten zur Interaktion mit dem Internet. Folglich sind Browser die Hauptangriffsziele für

Cyberangreifer. Verwenden Sie immer die neueste Version Ihres Browsers und halten Sie Ihr Sicherheitsschild gegen Browserangriffe stark. Aktualisierte Browser verfügen über die neuesten Sicherheits-Patches und sind für Cyber-Angreifer viel schwieriger auszunutzen. Sind Sie nicht sicher, ob Sie das neueste Browser-Update haben? Wenden Sie sich an den technischen Support oder das Informationssicherheitsteam, um dies zu überprüfen. Bleiben Sie online sicher, indem Sie keine Verbindung zu Websites herstellen, wenn Sie eine Warnung von Ihrem Browser erhalten. Moderne Browser können bestimmte bösartige Websites erkennen, die darauf abzielen, Schaden anzurichten. Wenn Ihr Browser Sie darauf hinweist, dass die Website, die Sie gerade besuchen wollen, gefährlich ist, schließen Sie diese Seite und versuchen Sie, die gesuchten Informationen auf einer sichereren Website zu finden. Vergewissern Sie sich, dass Ihr Browser HTTPS verwendet, was ein Zeichen für Verschlüsselung ist, bevor Sie sensible Daten online übermitteln, z. B. wenn Sie Ihre Kreditkartendaten beim Online-Einkauf angeben. Bei der Verschlüsselung werden die zwischen Ihrem Computer und dem Zielort übertragenen Informationen so vermischt, dass nur die autorisierte Website sie lesen kann. Achten Sie bei einer sicheren Verbindung auf Verschlüsselungszeichen wie die Website-Adresse, die mit HTTPS beginnt, und ein Vorhängeschloss-Symbol in der Statusleiste.

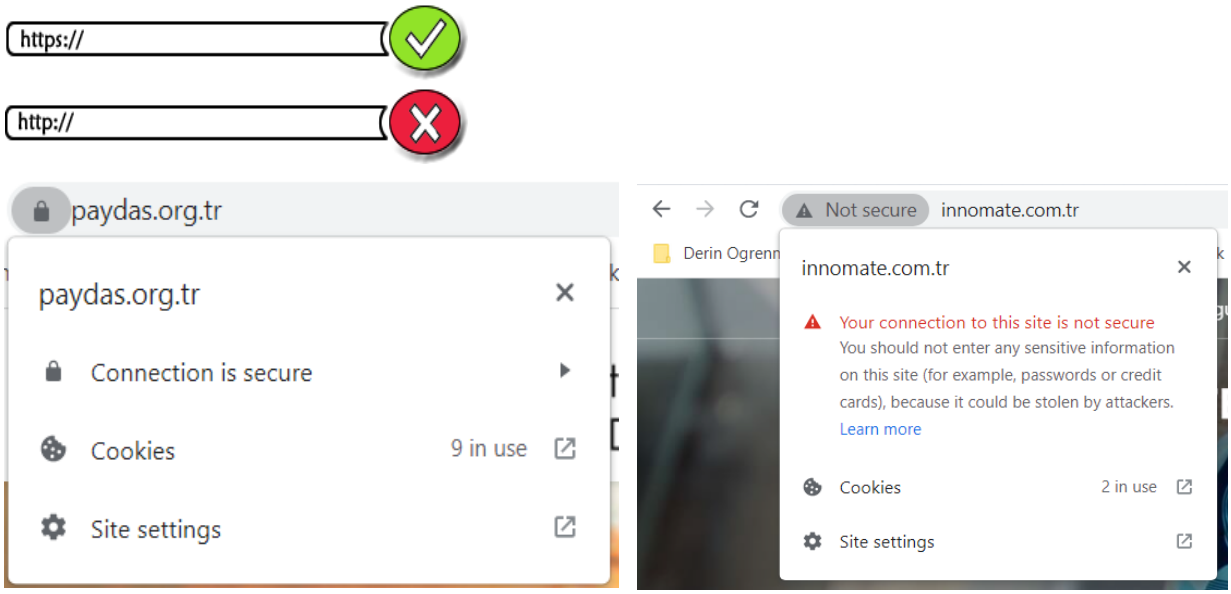


Abbildung 2. Sichere und nicht sichere Web-Sites

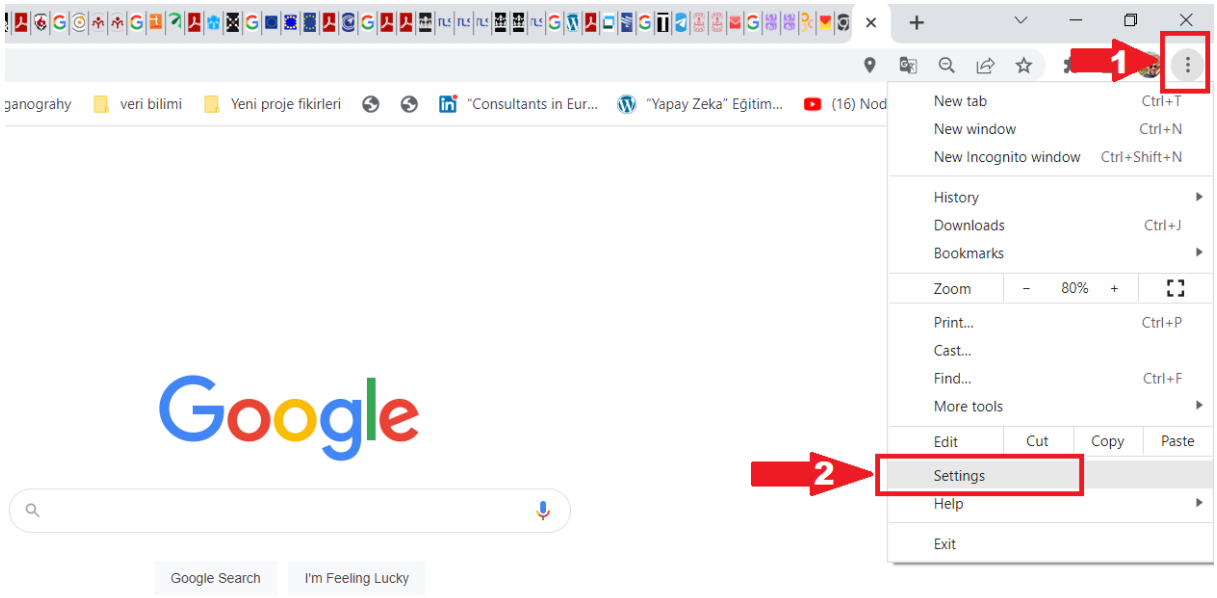
Add-ons; sind kleine Softwareteile, die zu Browsern hinzugefügt werden und für zusätzliche Funktionen wie Spiele, Filme oder Textbearbeitung verwendet werden. Jedes Add-on, das in Ihrem Browser installiert wird, kann zusätzliche Sicherheitslücken verursachen. Installieren Sie die Add-ons in Ihrem Browser nur, wenn Sie sie unbedingt benötigen, und nur nach vorheriger

Genehmigung. Verwenden Sie nach der Installation immer die neueste Version des Plug-ins, genau wie in Ihrem Browser. Vergewissern Sie sich schließlich, dass Sie nach dem Besuch einer Website abgemeldet sind. Dadurch werden sensible Anmelde- und Kennwortdaten vor dem Schließen des Browsers entfernt. Denken Sie daran, dass Ihr sicheres Surfverhalten und Ihr Sicherheitsschild dadurch gestärkt werden.

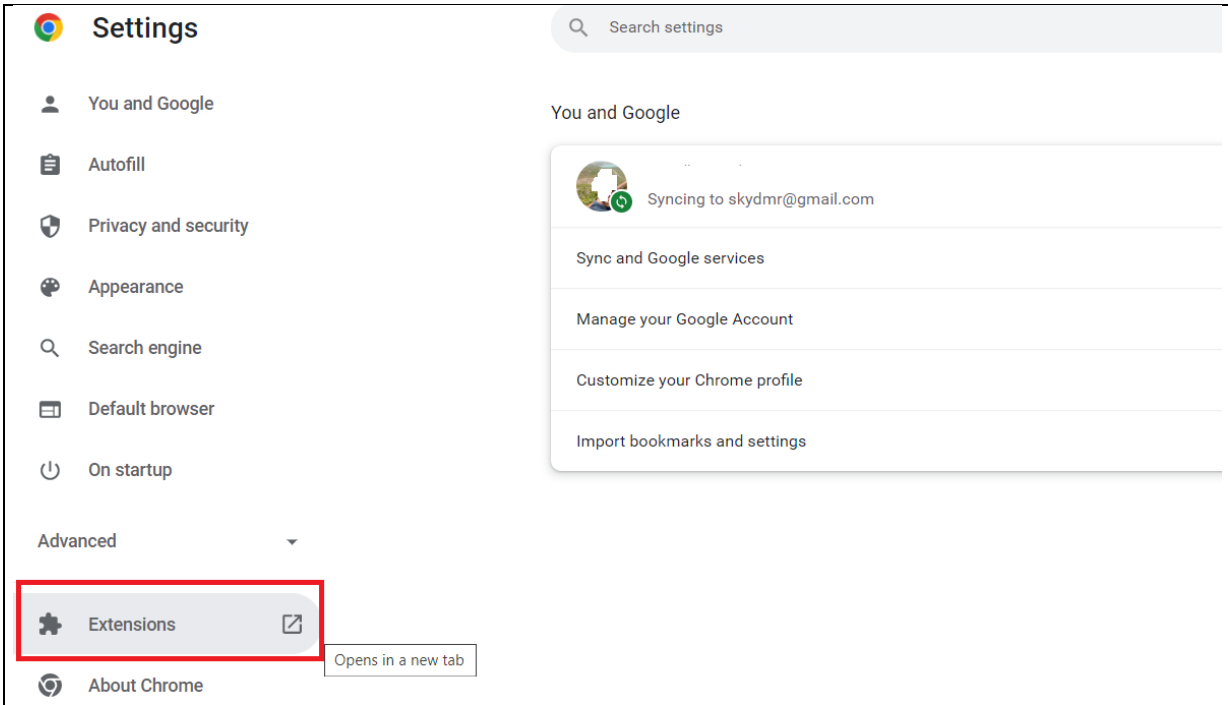
Übungen-3:

Führen Sie die folgenden Schritte aus, um Plug-ins im Webbrowser zu bearbeiten.

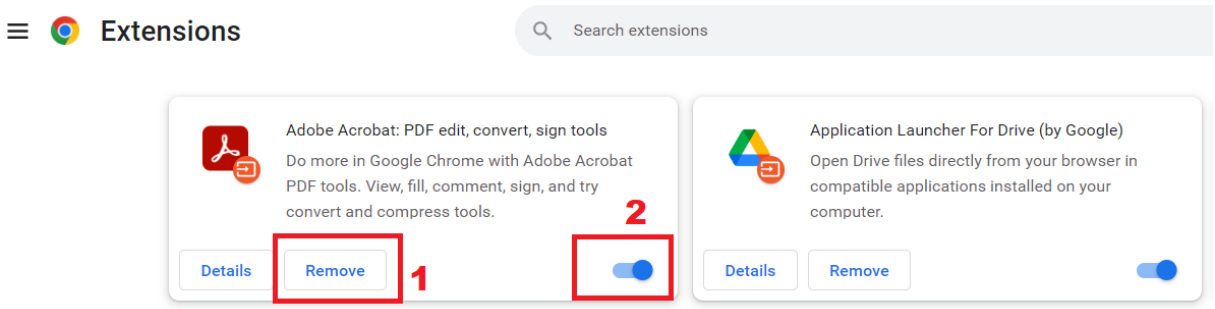
Schritt 1: Öffnen Sie Ihren Webbrowser und klicken Sie auf die Schaltfläche "Kostüm und Steuerung..." in der oberen linken Ecke (1). Klicken Sie auf die Registerkarte "Einstellungen" im Dropdown-Menü (2).



Schritt 2: Klicken Sie in dem sich öffnenden Fenster auf die Schaltfläche "Erweiterungen".



Schritt 3: Auf diesem Bildschirm sehen Sie die in Ihrem Browser installierten Add-ons. Wenn Sie das Add-on löschen möchten, können Sie es über die Schaltfläche "Entfernen" löschen (1). Wenn Sie möchten, dass das Plugin inaktiv bleibt, können Sie es über die Schaltfläche "Ein-Aus" deaktivieren (2).



4. E-Mail, Messaging und Phishing: Sie haben eine E-Mail in Ihrem Posteingang oder eine Nachricht auf Ihrem Telefon. "Es gibt ein Problem mit Ihrem Konto und Ihr Konto sollte sofort aktualisiert werden. Alles, was Sie tun müssen, ist auf einen Link zu klicken. Wenn Sie eine Nachricht mit Inhalt erhalten, halten Sie inne und denken Sie nach, bevor Sie klicken! "Phishing" ist ein Social-Engineering-Angriff, bei dem E-Mails oder Nachrichten als Köder verwendet werden, ähnlich wie beim Angeln. Cyber-Angreifer verschicken Tausende von E-Mails in der Hoffnung, dass jemand den Köder schluckt. In den E-Mails werden Sie aufgefordert, eine Aktion durchzuführen,

z. B. auf einen Link zu klicken, einen Anhang zu öffnen oder ein Formular auszufüllen. Die Cyber-Angreifer wissen nicht genau, wer diese E-Mails erhält, aber wenn Sie eine dieser scheinbar harmlosen Aktionen durchführen, könnten Sie in die Falle tappen. Eine raffiniertere Form des Phishings, das so genannte "Spear Phishing", zielt auf bestimmte Personen ab. Zum Beispiel, wenn jeder in unserem Unternehmen eine allgemeine Phishing-E-Mail über ein nicht zugestelltes Paket erhält, oder wenn fünf Personen in unserer Einkaufsabteilung mit einer gefälschten Rechnungsanforderung angesprochen werden. Woran erkennt man, dass es sich bei einer E-Mail oder Nachricht um einen Phishing-Angriff handelt?

Einige Anzeichen, auf die Sie achten sollten:

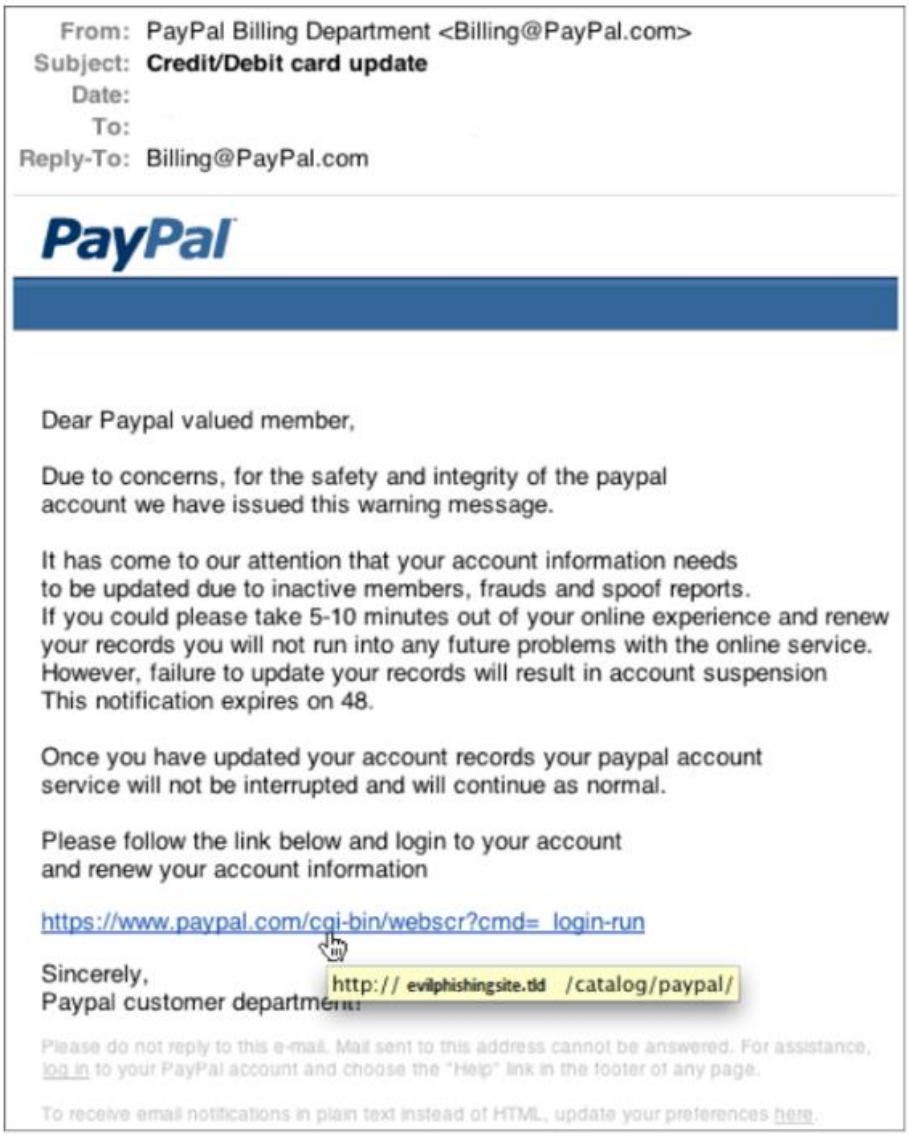
- Nachrichten, die mit "Sehr geehrter Kunde" oder anderen allgemeinen Begrüßungseinträgen beginnen.
- Nachrichten, die sofortiges Handeln erfordern oder ein Gefühl der Dringlichkeit vermitteln, wie z. B. die Drohung, Ihr Konto zu schließen.
- Nachrichten, die vorgeben, von einer offiziellen Organisation zu stammen, aber grammatikalische oder Rechtschreibfehler aufweisen oder eine persönliche E-Mail-Adresse wie @gmail.com, @yahoo.com oder @hotmail.com verwenden.
- Jede Nachricht, die nach hochsensiblen Informationen fragt, z. B. nach Ihrer Kreditkartennummer oder Ihrem Passwort. Seien Sie bei solchen Nachrichten misstrauisch. Wenn Ihnen jemand, den Sie kennen, z. B. ein Kollege, eine Nachricht schickt, die dringende Maßnahmen erfordert, sollten Sie sich über verschiedene Kanäle vergewissern, dass die Nachricht wirklich von ihm stammt, z. B. durch einen Telefonanruf.

Denken Sie daran, dass es für einen Cyberangreifer sehr einfach ist, eine E-Mail zu erstellen, die so aussieht, als käme sie von einem Freund oder Kollegen. Um sicher zu sein, sollten Sie bei der Verwendung von E-Mails oder Nachrichten immer die folgenden Vorsichtsmaßnahmen treffen. Fahren Sie mit der Maus über einen Link, bevor Sie ihn anklicken. Auf diese Weise wird das wahre Ziel des Links angezeigt, so dass Sie sich vergewissern können, dass Sie zu einer seriösen Website weitergeleitet wurden. Noch besser ist es, wenn Sie die Adresse der Website direkt in Ihren Browser eingeben. Wenn Sie zum Beispiel eine E-Mail von Ihrer Bank erhalten, in der Sie aufgefordert werden, Ihre Kontodaten zu aktualisieren, ignorieren Sie den per E-Mail zugesandten Link. Geben Sie einfach die Adresse der Website Ihrer Bank in Ihren Browser ein und melden Sie sich wie gewohnt an. Wenn Nachrichten Anhänge enthalten, öffnen Sie nur Anhänge, die Sie erwarten. Da Antivirenlösungen möglicherweise nicht alle Versionen von Malware

erkennen, sind Sie der beste Schutz vor infizierten Anhängen, den wir haben. Achten Sie bei der Verwendung von E-Mail oder Messaging darauf, dass Sie nicht versehentlich wichtige Informationen preisgeben. E-Mail-Funktionen wie die automatische Vervollständigung machen es leicht, versehentlich eine E-Mail an die falsche Person zu senden. Wenn Sie beispielsweise eine E-Mail an einen Mitarbeiter Ihres Referats senden möchten, kann es passieren, dass Sie versehentlich eine E-Mail an einen Freund mit einem ähnlichen Namen senden, der in einem anderen Referat arbeitet. Denken Sie daran, dass eine E-Mail, sobald sie versendet wurde, nicht mehr von Ihnen kontrolliert werden kann.

Beispiele für das Phishing

Beispiel 1: In diesem Beispiel sieht die E-Mail so aus, als käme sie von PayPal.com, wird aber über einen gefälschten Server verschickt. Wenn wir uns nur die Webadresse ansehen, an die sie gerichtet ist, ohne auf den angegebenen Link zu klicken, können wir erkennen, dass es sich um eine E-Mail handelt, die von einem Angreifer abgefangen wurde, der Anmeldedaten erhalten möchte.



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date:
To:
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

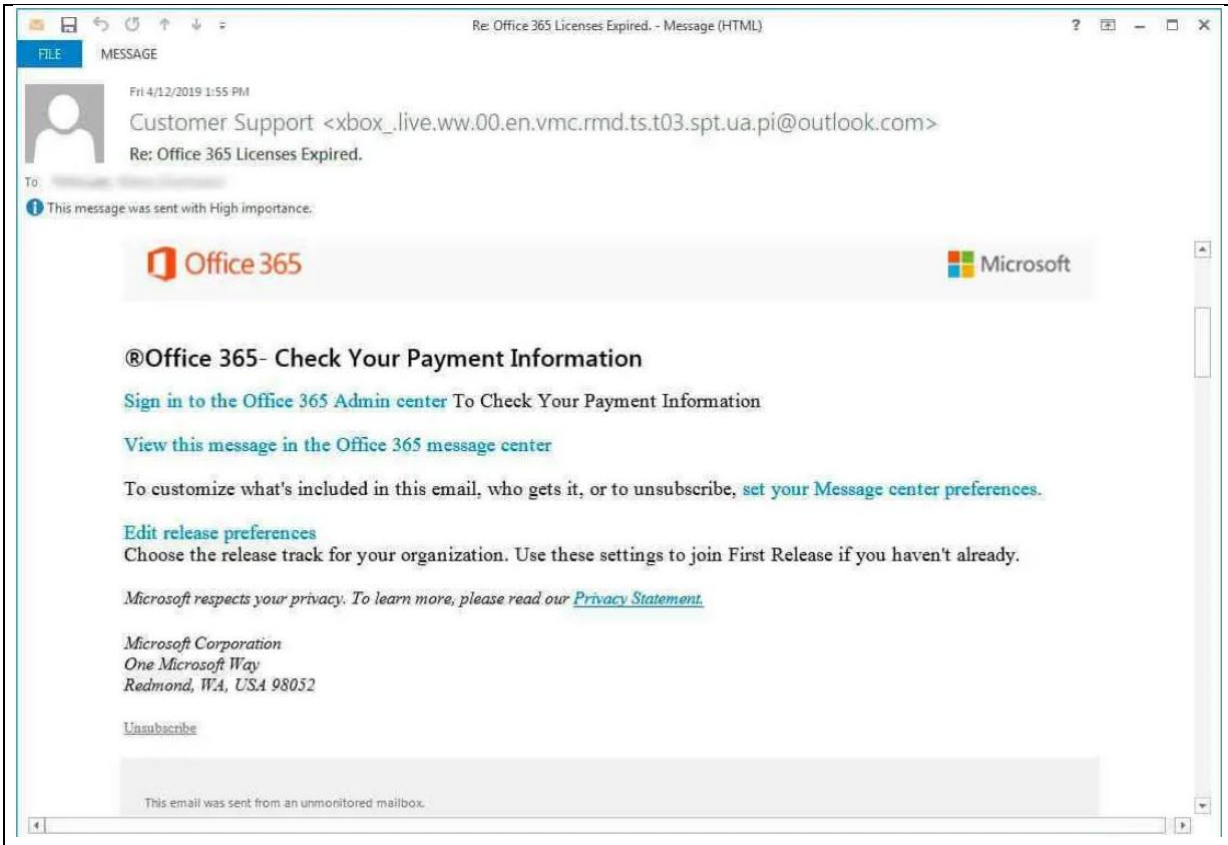
http:// evilphishingsite.tld /catalog/paypal/

Sincerely,
Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

Beispiel-2: In diesem Beispiel weist eine eingehende E-Mail darauf hin, dass die Office 365-Lizenzen einer Organisation abgelaufen sind. In der E-Mail wird der Benutzer dann aufgefordert, sich beim Office 365 Admin Center anzumelden, um seine Zahlungsinformationen zu überprüfen.



Bei genauer Prüfung der Absender-E-Mail-Adresse ist jedoch festzustellen, dass eine solche Adresse nicht existiert. Kurzum, es ist offensichtlich, dass diese E-Mail nicht von Office365 gesendet wurde.

5. Soziale Netzwerke

Soziale Netzwerke helfen uns, Informationen auszutauschen und mit anderen zu kommunizieren. Leider machen es diese Websites auch Cyber-Angreifern leichter, Sie aufzuspüren und herauszufinden, was Sie tun. Schützen Sie sich, indem Sie jedes Konto mit einem starken, eindeutigen Passwort schützen. Noch besser ist es, für jedes Konto ein anderes Passwort zu verwenden und, falls verfügbar, eine Zwei-Faktor-Authentifizierung einzusetzen. Viele Social-Networking-Sites unterstützen auch Apps von Drittanbietern. Installieren Sie nur Apps, die Sie benötigen, und nur aus vertrauenswürdigen Quellen. Überprüfen Sie die Bewertungen, Kommentare und Berechtigungen jeder App, bevor Sie sie installieren. Wenn Sie eine App nicht mehr benötigen, deinstallieren Sie sie oder deaktivieren Sie ihren Zugriff auf Ihr Profil in einem sozialen Netzwerk.

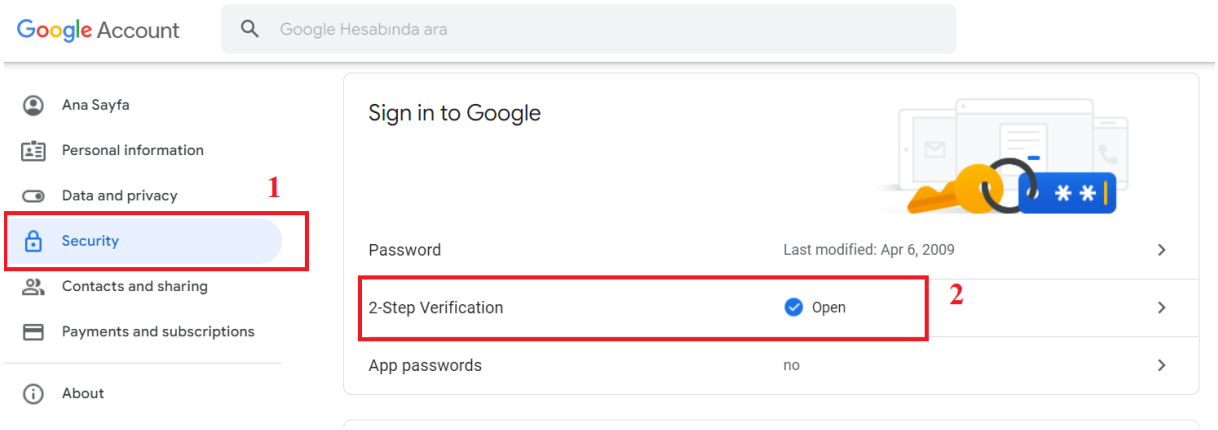
Genau wie bei E-Mail und Messaging können Cyber-Angreifer versuchen, Sie auf Social-Networking-Sites zu betrügen. Er kann Nachrichten senden, die vorgeben, Ihr Freund zu sein. Wenn Sie eine seltsame oder verdächtige Nachricht von einem Freund erhalten, kontaktieren Sie ihn per E-Mail oder Telefon, nicht indem Sie auf die Nachricht antworten. Um unsere Institution zu schützen, sollten Sie keine vertraulichen Informationen über unsere Institution auf irgendeiner Website veröffentlichen. Wenn Sie Fragen dazu haben, was Sie veröffentlichen oder über Ihre Arbeit mitteilen dürfen, wenden Sie sich bitte an Ihren Vorgesetzten.

Nachdem Sie die Zwei-Faktor-Authentifizierung (Verifizierung) aktiviert haben, wird jedes Mal, wenn Sie sich von einem neuen Gerät oder Browser aus bei Ihrem Konto anmelden, ein Sicherheitscode an Ihr Telefon oder Ihre Authentifizierungs-App gesendet. Sie müssen diesen Code eingeben, damit Sie sich anmelden können. Wenn ein Cyberkrimineller versucht, sich bei Ihrem Konto anzumelden, kann er dies nicht tun, wenn er keinen Zugriff auf Ihr Mobiltelefon hat. Sie können den Versuch, sich in Ihr Konto einzuloggen, auch daran erkennen, dass Sie eine Benachrichtigung mit einem Code erhalten. Teilen Sie diesen Code niemals mit anderen! Ein Angreifer wird versuchen, ihn zu stehlen. Wenn Sie den Code erhalten, aber nicht versucht haben, sich einzuloggen, löschen Sie die Code-Nachricht und ändern Sie Ihr Passwort so schnell wie möglich.

Übungen-4:

Führen Sie die Zwei-Faktor-Authentifizierung durch, um auf das von Ihnen erstellte E-Mail-Konto zuzugreifen. Der erste dieser Prozesse ist das Passwort, das Sie für den Zugriff auf das Konto verwenden. Das andere kann ein Verifizierungscode (SMS) sein, der an Ihr Telefon gesendet wird, oder ein Bestätigungslink, der an eine andere E-Mail-Adresse gesendet wird.
Der folgende Screenshot zeigt, wie Sie die Zwei-Faktor-Authentifizierung des Google Mail-Kontos aktivieren.
Schließen Sie den Vorgang ab und versuchen Sie erneut, auf Ihr E-Mail-Konto zuzugreifen.

Schritt 1: Öffnen Sie Ihr Google-Konto.
Schritt 2: Klicken Sie auf den Abschnitt "Einstellungen".
Schritt 3: Wählen Sie die Registerkarte "Sicherheit" aus dem Menü auf der linken Seite der sich öffnenden Seite (1). Aktivieren Sie dann die Funktion "2-Schritt-Verifizierung" in der Mitte der Seite.



1.7. Bewährte Verfahren für eine erfolgreiche Informationssicherheitspolitik

1. **Klassifizierung von Informationen und Daten:** Sie können über Ihr Sicherheitsprogramm entscheiden oder es zerstören. Eine unzureichende Informations- und Datenklassifizierung kann Ihre Systeme für Angriffe anfällig machen. Darüber hinaus kann eine ineffiziente Verwaltung von Ressourcen zu hohen Kosten führen. Eine klare Klassifizierungspolitik hilft Unternehmen, die Verteilung ihrer Sicherheitsressourcen zu kontrollieren.
2. **IT-Betrieb und Verwaltung:** Sie sollten zusammenarbeiten, um Compliance- und Sicherheitsanforderungen zu erfüllen. Mangelnde Zusammenarbeit zwischen den Abteilungen kann zu Konfigurationsfehlern führen. Teams, die zusammenarbeiten, können die Risikobewertung und -identifizierung durch alle Abteilungen koordinieren, um Risiken zu verringern.

3. **Reaktionsplan auf Sicherheitsvorfälle:** Hilft bei der Einleitung geeigneter Abhilfemaßnahmen bei Sicherheitsvorfällen. Eine Strategie für Sicherheitsvorfälle bietet einen Leitfaden, der eine erste Reaktion auf Bedrohungen, die Ermittlung von Prioritäten und geeignete Abhilfemaßnahmen umfasst.
4. **SaaS- und Cloud-Richtlinien** - geben dem Unternehmen klare Richtlinien für die Einführung von Cloud und SaaS, die die Grundlage für ein einheitliches Cloud-Ökosystem bilden können. Diese Richtlinie kann dazu beitragen, unwirksame Komplikationen und eine schlechte Nutzung von Cloud-Ressourcen zu vermeiden.
5. **Richtlinien zur akzeptablen Nutzung (AUPs):** Sie helfen dabei, Datenschutzverletzungen zu verhindern, die durch den Missbrauch von Unternehmensressourcen entstehen. Transparente AUPs tragen dazu bei, dass alle Mitarbeiter mit der ordnungsgemäßen Nutzung der Technologieressourcen des Unternehmens im Einklang stehen.
6. **Richtlinie für Identitätszugriff und -verwaltung (IAM):** Legt fest, wie IT-Administratoren Systeme und Anwendungen für die richtigen Mitarbeiter autorisieren und wie Mitarbeiter Passwörter erstellen, um die Sicherheitsstandards einzuhalten. Eine einfache Passwortrichtlinie kann Identitäts- und Zugriffsrisiken verringern.
7. **Datensicherheitspolitik:** Umreißt die technischen Anforderungen und akzeptablen Mindeststandards für die Datensicherheit zur Einhaltung der einschlägigen Gesetze und Vorschriften
8. **Datenschutzbestimmungen**: Von der Regierung durchgesetzte Vorschriften wie die Allgemeine Datenschutzverordnung (GDPR) schützen die Privatsphäre der Endnutzer. Organisationen, die die Privatsphäre ihrer Nutzer nicht schützen, riskieren den Verlust ihrer Befugnisse und können mit Geldstrafen belegt werden.
9. **Richtlinie für persönliche und mobile Geräte:** Legt fest, ob Mitarbeiter persönliche Geräte für den Zugriff auf die Unternehmensinfrastruktur verwenden dürfen und wie das Risiko einer Gefährdung durch mitarbeitereigene Geräte verringert werden kann. Heutzutage sind die meisten Unternehmen auf die Cloud umgestiegen. Unternehmen, die ihre Mitarbeiter ermutigen, von jedem beliebigen Ort aus auf Unternehmenssoftware zuzugreifen, riskieren, dass persönliche Geräte wie Laptops und Smartphones Schwachstellen aufweisen. Die Erstellung einer Richtlinie für die ordnungsgemäße Sicherung persönlicher Geräte kann dazu beitragen, die Gefährdung durch Bedrohungen über mitarbeitereigene Geräte zu verhindern.
10. **Richtlinie für den Fernzugriff**: Legt die zulässigen Methoden für den Fernzugriff auf interne Netzwerke fest.
11. **E-Mail-/Kommunikationsrichtlinie**: Legt fest, wie Mitarbeiter den vom Unternehmen gewählten elektronischen Kommunikationskanal wie E-Mail, Slack oder soziale Medien nutzen können.

12. **Richtlinie zur Wiederherstellung im Katastrophenfall**: Umreißt den Beitrag der Cybersicherheits- und IT-Teams des Unternehmens zu einem Gesamtplan für die Geschäftskontinuität
13. **Geschäftskontinuitätsplan (BCP):** Koordiniert die Bemühungen im gesamten Unternehmen und wird im Falle einer Katastrophe eingesetzt, um den Geschäftsbetrieb wiederherzustellen.
14. **Richtlinie zur Reaktion auf Vorfälle (IR)**: Ein organisierter Ansatz, wie die Organisation einen Vorfall bewältigen und beheben wird
15. **Änderungsmanagement-Richtlinie**: Bezieht sich auf den formalen Prozess für Änderungen an IT, Softwareentwicklung und Sicherheit

Fragen:

1- Was gehört nicht zu den Elementen der Informationssicherheit?

A) Vertraulichkeit

B) Integrität

C) Schwachstelle

D) Zugänglichkeit

2- Welche der folgenden Institutionen ist nicht für die Informationssicherheitspolitik zuständig?

A) ENISA

B) IPA

C) GDPR

D) NIST

3- Welcher der folgenden Vorteile hat keine direkten Auswirkungen auf die Informationssicherheit einer Organisation?

A) Schutz sensibler Daten

B) Minimierung des Risikos von Sicherheitsvorfällen

C) Bereitstellung einer eindeutigen Erklärung zur Sicherheit für Dritte

D) Verkürzung der Arbeitszeiten der Beschäftigten

4- Welcher der folgenden Punkte gehört nicht zur Informationssicherheit

A) Hardware-Politik

B) E-Mail-Richtlinie

C) Richtlinie zum Notfallwiederherstellungsplan

D) Passwortschutz-Richtlinie

5- Welches der folgenden Beispiele ist ein gut definiertes Passwort?

A) 20220829

B) InCyT#2021!

C) Erasmus+

D) 123456!

6- Welche der folgenden Maßnahmen gehört nicht zu den Maßnahmen, die zur Informationssicherheit ergriffen werden müssen?

A) Bevorzugen Sie https-Webseiten

B) Verwendung eines sicheren Passworts

C) Besuch von Links mit unbekanntem Ursprung

D) Höchstens 8 Stunden pro Tag auf den Computerbildschirm schauen

Fragen zur Selbsteinschätzung. Nach der Beantwortung kann der Lernende die Ergebnisse sehen und sie mit den auf der Plattform gespeicherten Ergebnissen vergleichen

- ***Warum ist eine Informationssicherheitspolitik wichtig?***

- ***Erklären Sie die Richtlinie zum Schutz von Passwörtern***

Anhänge (PowerPoint-Präsentation, Handouts, Ausdrucke, Links, Video...):

Referenzen:

http://bid.ankara.edu.tr/2018/10/02/siber-guvenlik-farkindaligi/
https://purplesec.us/resources/cyber-security-policy-templates/#Email
http://ix-one.com/domainhostingFAQ/article/MS_27805.html

https://www.siberguvenlik.web.tr/index.php/2019/07/22/kimlik-avcilari-sahte-yonetici-uyarilari-ile-office-365-yoneticilerini-hedefliyor/