Lerneinheit

[Cybersicherheit]

Projekt: B-SAFE
Nummer: 2018-1CZ01-KA204-048148

Funded by the
Erasmus+ Programme
of the European Union

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

Cybersicherheit

Einführung

Haben Sie einen böswilligen Angriff erlebt, bei dem zum Beispiel jemand versucht hat, ein wichtiges Dokument oder private Informationen über einen in einer E-Mail vorhandenen Link zu stehlen? Wenn Ihnen so etwas passiert ist, waren Sie Opfer der Cybersicherheit.

Heutzutage ist die Cybersicherheit ein großes Anliegen. **Bei der Cybersicherheit geht es darum, digitale Angriffe zu verhindern und zu erkennen und Systeme, Hardware und Software zu schützen.** Cybersicherheit bezieht sich auch auf die Vorbeugung, Erkennung, Reaktion und Behebung von Cybersicherheitsvorfällen, die beabsichtigt sein können oder nicht. Normalerweise zielen Cyberangriffe darauf ab, **auf Daten/Informationen zuzugreifen, sie zu verändern, zu stehlen oder zu zerstören, Geld zu erpressen oder normale Geschäfte und kritische Infrastrukturen zu unterbrechen.** Wussten Sie, dass laut neueren Studien die Gesamtkosten der Cyberkriminalität für jedes Unternehmen etwa 12.000.000€ betragen?

Daher ist die Cybersicherheit eine aktuelle Debatte, die die Gesellschaft als Ganzes einbeziehen muss, da jeder Mensch eine wichtige Rolle beim Schutz seiner eigenen digitalen Informationen spielt.

Praktische Relevanz - Hierfür benötigen Sie das Wissen und die Fähigkeiten

Cyberangriffe finden ständig statt, was bedeutet, dass es wichtiger denn je ist, Software, Hardware und Daten sicher zu verwahren und zu schützen. Trotzdem gibt es nur wenige Menschen, die über diese Fähigkeiten verfügen. Wenn Sie also lernen, wie Sie in die Cybersicherheit einsteigen können, kann Ihnen das bei Ihrer eigenen persönlichen Internetsicherheit helfen.
Nach dem Erlernen dieser Inhaltseinheit werden Sie mit dem Begriff Cybersicherheit in Berührung kommen und erfahren, warum Cybersicherheit heutzutage so wichtig ist. Darüber hinaus werden Sie in dieser Lerneinheit wissen, was Sie tun können, um in Ihrem täglichen Leben einige Maßnahmen zur Cybersicherheit zu ergreifen.

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

1.Wissen aufbauen - Cybersicherheit - Definition und Gesetzgebung

Datenschutz und Cybersicherheit werden zu wesentlichen Werten für die Gesellschaft. Aus diesem Grund haben diese beiden Bereiche in jüngster Zeit eine bedeutende rechtliche Entwicklung durchlaufen und sind nun in der EU stärker konsolidiert. Die Beseitigung von Bedrohungen und Cyberangriffen ist jedoch nahezu unmöglich, so dass der Einsatz von Cybersicherheitsmaßnahmen und verstärkten Cybersicherheitskapazitäten obligatorisch ist.

Die Umsetzung wirksamer Cybersicherheitsmaßnahmen ist heute eine besondere Herausforderung, da es mehr Geräte als Menschen gibt und Hacker immer innovativer werden. In der heutigen vernetzten Welt profitieren alle von fortschrittlichen Cybersicherheitsmaßnahmen. Auf individueller Ebene kann ein Cyberangriff alles Mögliche zur Folge haben, vom Identitätsdiebstahl über Erpressungsversuche bis hin zum Verlust wichtiger Daten.

Aber was genau verstehen wir unter "Cybersicherheit"?

Definition
Cybersicherheit ist die Praxis **der Verteidigung von Computern, Servern, mobilen Geräten, elektronischen Systemen, Programmen, Netzwerken und Daten vor böswilligen Angriffen, Schäden oder unbefugtem Zugriff**. Es gibt keine einheitliche, insbesondere keine allgemein akzeptierte Definition von Cybersicherheit. Mit anderen Worten: Cybersicherheit bezieht sich auf alle Schutzmaßnahmen und Vorkehrungen, die zur Verteidigung von Informationssystemen und ihrer Nutzung gegen unbefugten Zugang, Angriffe und Schäden getroffen werden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.

1.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was ist die Bedeutung von Cybersicherheit?

Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Cybersicherheit umfasst die Verteidigung von Hardware und Software.
- Cyberangriffe nehmen zu, und jeder ist heute anfälliger für diese Art von Vorfällen.
- Wirksame Cybersicherheitsmaßnahmen umfassen die Anwendung mehrerer Cybersicherheitsmaßnahmen.
- Aufgrund der Notwendigkeit der Anwendung mehrerer Cybersicherheitsmaßnahmen sollten so früh wie möglich Schulungen zur Cybersicherheit durchgeführt werden.

2.Wissen aufbauen - Cybersicherheit - Passwortsicherheit

Kennen Sie den einfachsten Weg für einen Cyberkriminellen, Zugang zu Ihrer Bank, sozialen Medien, E-Mail und anderen privaten Daten zu erhalten? Es ist ein **schwaches Passwort**. Tatsächlich werden die meisten Passwörter in einem "Wimpernschlag" geknackt. Laut dem Nacional Cyber Security Centre waren die fünf häufigsten Passwörter im Jahr 2019 "123456", "123456789", "qwerty", "password" und "1111111". Wenn Sie also einige dieser oder ähnliche Passwörter haben, sehen Sie sich bitte das folgende Beispiel an.

Beispiel

Zeitaufwand zum Knacken von Passwörtern

123456	0,29 ms
potato	1,37 ms
Potato	3,28 s
P0tat0	1h 23m.27s 0.10ms
P0tat0!	1 Monat, 3 Wochen, 5 Tage und 21h 54min, 40s 8ms
IAtE27P0taT0s!	47623938 Jahrtausende, 8 Jahrhunderte, 73 Jahre und 8 Monate

Eines der häufigsten Probleme mit Passwörtern ist, dass sie im Allgemeinen leicht zu erraten sind. Viele Leute denken, dass ein kurzes Passwort mit vielen verschiedenen Zeichentypen sicher ist, obwohl in Wirklichkeit die einzige Möglichkeit, ein wirklich sicheres Passwort zu gewährleisten, darin besteht, **mindestens 14 Zeichen lang und etwas willkürlich zu machen**. Außerdem ist es, wie Sie sehen können, **umso schwieriger zu erraten, je komplexer Ihr Passwort ist**. Ein sicheres Passwort ist eine Kombination

aus Buchstaben (Groß- und Kleinbuchstaben), Zahlen und Symbolen. Eine gute Möglichkeit, Ihr einzigartiges Passwort nie zu vergessen, besteht darin, einen Satz anstelle von Wörtern zu wählen und ihn mit alphanumerischen Zeichen zu mischen - die meisten Websites erlauben sogar Leerzeichen zwischen den Wörtern!

Nichtsdestotrotz gibt es noch weitere Aspekte zu beachten, wenn Sie neue Konten und digitale Profile erstellen, um Ihre Cybersicherheit und Ihren Cyberschutz vollständig zu maximieren. Im Folgenden können Sie sehr häufige "DOs" und "DON'Ts" (was man tun und nicht tun sollte in Bezug auf Passwörter beobachten. Wenn Sie diese "goldenen Regeln" befolgen, sind Ihre Passwörter für Hacker fast nicht zu entziffern.

DON'T: Verwenden Sie für jedes Konto dasselbe Passwort
DO: Eindeutige Passwörter zu eindeutigen Konten und Profilen erstellen

Wir alle wissen, dass heutzutage fast jede Website ein Konto erfordert und dass fast jeder für verschiedene Konten die gleichen Passwörter verwendet. Oft wird jedoch vergessen, dass diese Konten Identitäts- oder Finanzinformationen enthalten, die gestohlen oder kompromittiert werden können, und durch die Verwendung nur eines Passworts werden Sie ein leichtes Ziel für Cyberattacken.

DON'T: Speichern Sie Ihre Passwörter in einer anderen Quelle
DO: Merken Sie sich Ihre Passwörter und richten Sie Sicherheitsfragen zu Ihren Konten ein

Eine einfache Methode, die oft verwendet wird, um sich Passwörter zu merken, ist die Speicherung in einer Tabellenkalkulation, auf der Festplatte oder in persönlichen Notizen. Versuchen Sie, sich Ihre Passwörter zu merken! Als Vorsichtsmaßnahme können Sie auch Sicherheitsfragen für Ihre Konten einrichten. Verwenden Sie jedoch statt der üblichen Fragen wie "Wie heißt Ihre Mutter?" oder "Woher kommen Sie?" Fragen, die nur Sie beantworten können.

DON'T: Passwörter mit anderen teilen
DO: Seien Sie geheimnisvoll mit Ihren Passwörtern

Gleich nach der Verwendung desselben Passworts für jedes Konto wird ein weiterer häufiger Fehler damit in Verbindung gebracht, dass Menschen ihre Passwörter per E-Mail, Textnachrichten oder soziale Medien mit anderen teilen.
Um Ihre Passwörter sicher aufzubewahren, müssen Sie die Passwörter regelmässig ändern. Denken Sie daran, dass es irgendwo auf der Welt einen Hacker gibt, der immer wieder versucht, die Passwörter von Benutzern zu stehlen, und je mehr Zeit sie haben, desto größer ist das Risiko, dass sie Erfolg haben.

DON'T: Wählen Sie ein sicheres Kennwort und bleiben Sie dabei
DO: Ändern Sie Ihre Passwörter alle drei Monate

In den meisten Browsern und Anwendungen können die Benutzer ihre Anmeldedaten speichern, so dass sie diese nicht jedes Mal eingeben müssen, wenn sie sich anmelden wollen. Obwohl es sehr praktisch ist, sollten Sie daran denken, dass, wenn Sie Ihre Geräte verlieren und ein Fremder es schafft, Ihr Zugangspasswort zu knacken, alle diese Informationen für diese Person zugänglich sind.

DON'T: Einen Authentifizierungsfaktor verwenden
DO: Hinzufügen einer Zwei-Faktor-Authentifizierung für jedes digitale Konto

Wenn Sie die Zwei-Faktor-Authentifizierung für Ihre digitalen Konten verwenden, wird ihnen eine zusätzliche Sicherheitsebene hinzugefügt. Wenn sich jemand von einem neuen Standort, einem neuen

Gerät oder einem neuen Browser in Ihr Konto einloggt, erhalten Sie ein **Passwort**, das für die Anmeldung in Ihrem Konto eingegeben werden muss. Abgesehen davon ist eine andere Art der Zwei-Faktor-Authentifizierung ein **Fingerabdruck, ein Stimmabdruck oder ein Code**, der an Ihr Telefon gesendet wird. Viele Leute denken, dass dies zeitaufwendig ist, aber wenn Sie ernsthaft um Ihre Privatsphäre besorgt sind, sollten Sie eine Zwei-Faktor-Authentifizierung für Ihre digitalen Konten verwenden, wenn diese Option möglich ist. Wenn Sie nicht die Möglichkeit haben, eine Zwei-Faktor-Authentifizierung zu verwenden, sollten Sie die zuvor genannten Empfehlungen befolgen.

2.Wissen anwenden

Übung SINGLE CHOICE

Situation: Bitte wählen Sie aus den folgenden Sätzen den richtigen aus.
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip: nur ein Satz ist wahr.

- Es wird empfohlen, ein einfaches Passwort zu wählen, um es sich besser merken zu können.
- Einige eindeutige Passwörter sind von einem Vornamen, dem Namen eines Familienmitglieds oder dem Namen eines Haustiers abgeleitet.
- Je mehr Zeichen und Symbole die Passwörter enthalten, desto weniger schwer sind sie zu erraten.
- Ein sicheres Passwort besteht aus einer Kombination von Groß- und Kleinbuchstaben, Symbolen und Zahlen und ist mindestens acht Zeichen lang.

Übung MULTIPLE CHOICE

Situation: Was sind einige der Regeln zum Schutz Ihrer digitalen Konten vor Cyberangriffen?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Verwenden Sie dasselbe Passwort in mehreren Websites/Accounts.
- Ändern Sie die Passwörter regelmäßig.
- Speichern Sie die Anmeldedaten im Browser oder in der Anwendung eines bestimmten Computers.
- Ein Fingerabdruck, ein Stimmabdruck oder ein Pincode sind eine gute Wahl für eine Zwei-Faktor-Authentifizierung.
- Vermeiden Sie beim Erstellen eines neuen Passworts Wörter aus dem Wörterbuch, Pronomen, Benutzernamen und andere vordefinierte Begriffe sowie häufig verwendete Passwörter.

3.Wissen aufbauen - Online-Shopping

Wie wir bereits gesehen haben, entwickelt sich bei der Cybersicherheit die Verbindung zwischen Menschen und der Anwendung von Praktiken, die darauf abzielen, Informationen vor böswilligen Angriffen zu schützen.

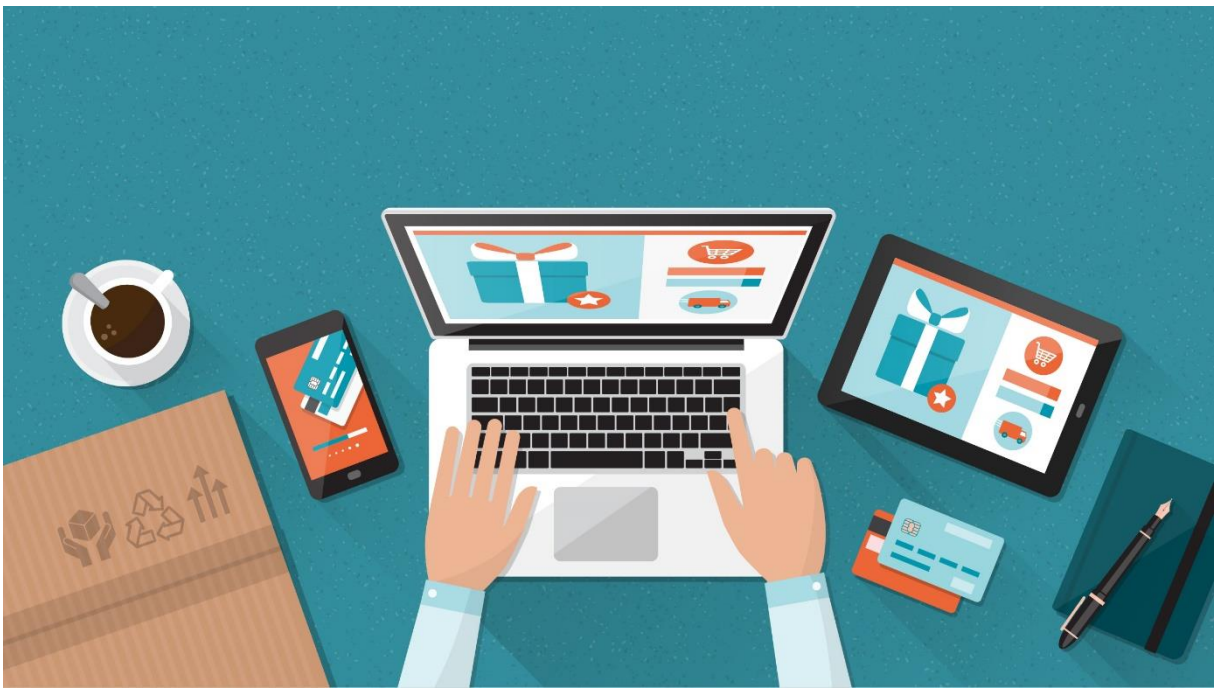
Im Jahr 2019 war der E-Commerce für rund 3,5 Billionen Dollar Umsatz verantwortlich und wird bis 2021 voraussichtlich 4,9 Billionen Dollar erreichen. Darüber hinaus kaufen 21,8% der Bevölkerung weltweit online ein, und Marken werden immer aktiver in sozialen Medien, was bedeutet, dass sie über verschiedene Online-Kanäle mehr und mehr mit den Menschen in Kontakt treten.

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

Heutzutage ziehen immer mehr Menschen das Online-Shopping dem konventionellen Einkaufen vor. Einige dieser Vorteile beziehen sich auf die Bequemlichkeit, Preisvergleiche, den Komfort und die Zugänglichkeit. Wenn Sie online einkaufen, müssen Sie in der Regel ein Konto einrichten. Folglich sind Sie verpflichtet, einige Ihrer persönlichen Daten anzugeben, wie "Name", "Adresse", "Telefonnummer", "E-Mail" und eine Zahlungsweise.

Vor diesem Hintergrund und weil alles im Internet verfolgt wird, ist es keine Überraschung, dass alle Daten, die sich aus der enormen Menge des elektronischen Handels und der Interaktionen in sozialen Medien ergeben, bedeuten, dass es wichtig ist, die möglichen Folgen dieser Handlungen genauer zu kennen.

Wenn Sie Internet-Betrügereien beim Online-Einkauf vermeiden wollen, müssen Sie einige Vorsichtsmaßnahmen ergreifen. Im Folgenden finden Sie einige Vorschläge:



Wissen, mit wem Sie es zu tun haben: Lesen Sie Rezensionen und sehen Sie nach, ob andere Verbraucher eine positive oder negative Erfahrung mit der Website gemacht haben. Stellen Sie sicher, dass die Website sicher ist.

Überwachen Sie Ihre Finanzkonten: Lesen Sie Ihre Aussagen regelmäßig und vergewissern Sie sich, dass sie die von Ihnen genehmigten Gebühren widerspiegeln.

Mit Kredit- oder Kundenkarte bezahlen: Kreditkarten sind im Allgemeinen die sicherste Option, da sie es Käufern ermöglichen, einen Kredit beim Herausgeber zu beantragen, wenn das Produkt nicht geliefert wird oder nicht dem entspricht, was bestellt wurde. Erwägen Sie die Verwendung einer virtuellen Einmal-Kreditkarte. Virtuelle Kreditkarten sind einmalige Kreditkarten, die es Ihnen ermöglichen, Transaktionen über Ihr Hauptkreditkartenkonto abzuwickeln, ohne Ihre Hauptkreditkarten-Kontonummer zu verwenden oder preiszugeben. Sie können zum Beispiel Capital One verwenden, um diese Art von Kreditkarten zu erstellen.

Sehen Sie sich die Datenschutzrichtlinie an: Die Datenschutzrichtlinie beschreibt, wie Ihre persönlichen Daten erfasst, verwendet und weitergegeben werden, wenn Sie einen Online-Shop

besuchen oder dort einen Kauf tätigen. Sie sollten die Datenschutzrichtlinie lesen und prüfen, ob Sie mit dem Datenschutz des Unternehmens einverstanden sind.

Kostenlos kann teuer sein: Kostenlose Bildschirmschoner, E-Cards oder andere können gefährliche Viren enthalten. Halten Sie Ihre Antiviren- und Anti-Spyware-Software zusammen mit Ihrer Firewall auf dem neuesten Stand.

Schicken Sie Ihre Finanzinformationen nicht per E-Mail: Legitime Unternehmen fragen nicht per E-Mail oder Pop-up-Nachricht nach finanziellen Informationen.

3.Wissen anwenden

Übung MULTIPLE CHOICE

Situation: Was sind einige der Informationen, die Sie beim Online-Shopping niemals angeben sollten?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Sozialversicherungsnummer
- Sicherheitscode der Kreditkarte (PIN)
- Nummer der Debitkarte
- Bankkontonummer
- E-Mail-Adresse

Übung MULTIPLE CHOICE

Situation: Bitte wählen Sie aus der Liste die richtigen Verhaltensweisen aus, um nicht Opfer von Cyberkriminalität zu werden
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Bevor die Kreditkarteninformationen angegeben werden, muss genügend Zeit für die Recherche auf der Website eingeplant werden.
- Kaufen Sie von einer Website, die über eine Verschlüsselung verfügt.
- Lesen Sie die Rückgabebestimmungen und andere Geschäftsbedingungen der Website sowie die Datenschutzrichtlinie der Website, bevor Sie etwas bestellen.
- Bezahlen Sie mit einer Debitkarte, in bar oder per Überweisung.
- Verwenden Sie einen "Hotspot", um Ihre Vertraulichkeit zu schützen.

4.Wissen aufbauen - Cloud Computing

Längst vorbei sind die Zeiten, in denen Sie Ihre Dateien auf einer Compact Disc oder sogar auf einem Pen Drive gespeichert haben, immer mit dem schrecklichen Gefühl, dass Sie diese schließlich verlegen würden, um nie wieder gefunden zu werden. Heutzutage können Sie von jedem Computer aus auf Ihre Dateien zugreifen, und in der Tat werden Cloud-Lösungen derzeit weltweit immer häufiger für alltägliche Aktivitäten genutzt.

Sie interagieren ständig mit einer Art von Cloud-Lösungen, wenn Sie Ihre E-Mails abrufen oder während Sie Ihr Telefon benutzen, um die Verkehrsbedingungen zu überprüfen. **Bei Cloud-Lösungen werden Ihre Daten bei einem Provider gespeichert und über das Internet abgerufen.**

Daher stellt sich in diesem Zusammenhang die Frage, ob unsere Daten in der Wolke sicher und geschützt sind. Aus diesem Grund ist es wichtig, mehr über das Konzept des Cloud Computing zu wissen.

Definition **Cloud Computing** kann definiert werden durch die **Bereitstellung von IT-Ressourcen** auf Abruf - wie z.B. Speicher, Rechenleistung oder Kapazität zur gemeinsamen Nutzung von Daten - über das Internet durch Hosting auf entfernten Servern. Mit anderen Worten bedeutet Cloud Computing die Speicherung von und den Zugriff auf Daten und Programme über das Internet anstelle der Festplatte Ihres Computers. Zu diesen Ressourcen gehören Tools und Anwendungen wie Datenspeicherung, Server, Datenbanken, Netzwerke und Software. Cloud-Lösungen sind eine sehr beliebte Option für Menschen und Unternehmen aus einer Reihe von Gründen, darunter Kosteneinsparungen, erhöhte Produktivität, Geschwindigkeit und Effizienz, Leistung und Sicherheit.

Die Wolke, die großen Datenmengen und die Digitalisierung der Industrie gehen einher mit einer zunehmenden Aufdeckung von Schwachstellen, wodurch böswillige Menschen noch mehr Opfer ins Visier nehmen können. Die Vielfalt der Angriffstypen und ihre zunehmende Raffinesse machen es wirklich schwierig, Schritt zu halten. **Aus diesem Grund ist es wichtig, einige tägliche Vorsichtsmassnahmen zu treffen, um Diebstahl, Durchsickern und/oder Löschen wichtiger Informationen zu vermeiden.**

Hier finden Sie eine kurze Zusammenfassung einiger Maßnahmen, die Sie einsetzen können, um die Sicherheit beim Cloud Computing zu verbessern.

	Die herkömmliche Kombination aus Benutzernamen und Passwörtern reicht oft nicht aus, um Benutzerkonten vor Hackern zu schützen, und gestohlene Zugangsdaten sind eine der wichtigsten Methoden, mit denen Hacker Zugang zu Ihren Daten/Informationen erhalten.

Verwenden Sie eine Multi-Faktor-Authentifizierung	Aus diesem Grund müssen Sie nicht nur **starke Passwörter**, sondern auch eine **Multi-Faktor-Authentifizierung** - auch bekannt als Zwei-Faktor-Authentifizierung - verwenden, um sicherzustellen, dass sich nur autorisiertes Personal in Ihre Cloud-Anwendungen einloggen und auf diese sensiblen Daten zugreifen kann. Eine Multi-Faktor-Authentifizierung ist eine der effektivsten Methoden, um Hackern den Zugriff auf Ihre Cloud-Anwendungen zu verwehren. Einige Beispiele für die Multi-Faktor-Authentifizierung sind ein Passwort in Kombination mit einem über SMS versandten Code oder einer von einer Anwendung generierten Nummer. Es ist auch wichtig, dass Sie immer daran denken, sich abzumelden und niemals Ihre Zugangsdaten zu speichern.
Verwalten Sie Ihren Benutzerzugriff, um die Sicherheit beim Cloud Computing zu verbessern	Die meisten Menschen brauchen nicht zu jeder Information, jedem Antrag oder jeder Akte Zugang. Daher wird durch das Setzen entsprechender **Berechtigungsstufen sichergestellt**, dass jede Person nur die Anwendungen oder Daten/Informationen einsehen oder manipulieren kann. Wenn jemand Zugriff auf alles hat und von einer Phishing-E-Mail ausgetrickst wird und versehentlich seine Anmeldedaten angibt, hat der Hacker sehr leicht Zugang zu allen Informationen.
Überwachen, protokollieren und analysieren Sie Benutzeraktivitäten mit automatisierten Lösungen zur Erkennung von Eindringlingen	**Die Echtzeit-Überwachung und -Analyse von Benutzeraktivitäten** kann Ihnen helfen, eventuelle Unregelmäßigkeiten, die von normalen Verhaltensweisen/Mustern abweichen, zu erkennen. Diese ungewöhnlichen Aktivitäten könnten auf einen Bruch in Ihrem System hinweisen, so dass ein frühzeitiges Abfangen dieser Aktivitäten Hacker in ihrer Spur stoppen und Ihnen ermöglichen kann, Sicherheitsprobleme zu beheben, bevor etwas schief geht. Sie können viele Lösungen für die automatisierte 24/7-Netzwerküberwachung und -verwaltung finden und zu fortgeschrittenen Cybersicherheitslösungen aufsteigen. Da jedes Unternehmen/jede Person unterschiedliche Bedürfnisse für verschiedene Stufen der

	Cybersicherheit hat, sollten Sie sich einen dritten Teil zur Risikobewertung besorgen, bevor Sie eine große Investition tätigen.
Anti-Phishing-Ausbildung	Hacker können sich Zugang zu sicheren Informationen verschaffen, indem sie durch einige Techniken wie Phishing, Spoofing von Websites und Spionage in sozialen Medien Zugangsdaten stehlen. Denken Sie deshalb daran, dass z.B. **Phishing-Schulungen** ein kontinuierlicher Prozess sein sollten, der von jemandem geleitet werden muss, der mit der Organisation zusammenarbeitet, um ihn effektiv zu gestalten.
Sichern von Dateien in verschiedenen Cloud-Accounts	Unabhängig von Größenordnung, Branche, Region und/oder Menschen ist die Sicherstellung der Datenverfügbarkeit für jeden eine Priorität. Hinzu kommt, dass der Verlust von Daten/Informationen durch menschliches Versagen sehr hoch ist, also legen Sie nicht alle wichtigen Daten an einem Ort ab. Ganz gleich, ob Sie die Dateien auf Ihrem persönlichen Laptop schützen und darauf zugreifen oder ob Sie ein Managed Service Provider sind, der für ein Portfolio von Unternehmen (und deren wachsende Datenmengen) verantwortlich ist, Cloud-Anwendungen sind in der modernen digitalen Welt unverzichtbar. Daher ist es entscheidend, **mehr als eine Cloud-zu-Cloud-Backup-Lösung zu finden**, um sicherzustellen, dass eine Kopie der von Ihnen erstellten, gespeicherten und gemeinsam genutzten Daten an einem sicheren Ort aufbewahrt wird.

4. Wissen anwenden

Übung SINGLE CHOICE

Situation: Welche Aussage ist in Bezug auf Cloud Computing wahr?
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip: nur ein Satz ist wahr.

- Bei Platform as a Service (PaaS) bezahlt ein Unternehmen für Dienste wie Speicherung, Vernetzung und Virtualisierung nach dem Prinzip "Pay-as-the-go".

- Infrastructure as a Service (IaaS) ist ein Cloud-Computing-Modell, bei dem ein Drittanbieter Hardware- und Software-Tools bereitstellt Bankkontonummer
- Software as a Service (SaaS) ist ein Software-Lizenzierungs- und Bereitstellungsmodell, bei dem Software auf Abonnementbasis lizenziert und zentral gehostet wird.
- Bei der Nutzung von Cloud-Computern müssen Benutzer und Unternehmen physische Server verwalten.

Übung MULTIPLE CHOICE

Situation: Bitte wählen Sie aus der Liste die richtigen Verhaltensweisen aus, um nicht Opfer von Cyberkriminalität zu werden
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Speichern Sie Informationen wie Adressen, Telefonnummern, Bankinformationen usw. in verschiedenen Wolken.
- Erstellen Sie ein eindeutiges Passwort nur für den Cloud-Service.
- Bei der Verwendung von Cloud-Lösungen ist es nicht relevant, einen Virenschutz zu haben.
- Wegen seiner Bequemlichkeit wird empfohlen, die Anmeldedaten in der entsprechenden Anwendung zu speichern.

Quellen

Alexandra, Susan (April 04, 2019). 10 Tips for Keeping Your Personal Data Safe on Social Media. Retrieved from https://securitytoday.com/Articles/2019/04/04/10-Tips-for-Keeping-Your-Personal-Data-Safe-on-Social-Media.aspx?Page=2

Cucu, Paul (December 21, 2016). 17 Underused Online Shopping Security Tips. Retrieved from https://heimdalsecurity.com/blog/online-shopping-security-tips/

European Commission (March 2019). Briefing Paper: Challenges to effective EU cybersecurity policy, Briefing paper. European Court of Auditors.

Federal Trade Comission (n.d.). 9 Online Shopping Tips. Retrieved from https://www.yumpu.com/en/document/read/4010016/nine-online-shopping-tips-federal-trade-commission

Kapiswe, Subham (April 23, 2019). NCSC Reveals List Of World's Most Hacked Passwords. .Retrieved from https://en.wikipedia.org/wiki/List_of_the_most_common_passwords#cite_note-NCSCList-15

Kapersky (n.d.). Safer Online Shopping. Retrieved from https://usa.kaspersky.com/resource-center/preemptive-safety/online-shopping

National Cybersecurity Alliance (n.d.). Online Safety Basics: Online Shopping. Retrieved from https://staysafeonline.org/stay-safe-online/online-safety-basics/online-shopping/

Acronis (n.d.). Case study: The Benefits of Cloud-to-Cloud Backup Solutions from Acronis. Retrieved from https://www.acronis.com/en-us/articles/cloud-to-cloud-backup/

D'Silva, Frank (June 15, 2020). 6 Tips for Improving Cloud Computing Security. Retrieved from https://www.ntiva.com/blog/6-tips-for-improving-cloud-computing-security

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

Wissen sichern

Das Zeitalter des Internets gab uns die Supermacht der Allgegenwart. Es verringerte die Kluft zwischen Menschen, Unternehmen und Orten und ermöglichte es den Menschen, überall und mit jedem mit nur einem Klick zu sein.

Wie Sie in dieser Inhaltseinheit gelernt haben, liegt die Verantwortung für den **Online-Datenschutz und die Sicherheit persönlicher Daten bei allen Beteiligten**: Regierung, Software-Entwickler, Anbieter von Cloud-Diensten, Unternehmen und Endbenutzer.

Mit der Umsetzung des GDPR gewinnen die Endbenutzer Vertrauen in ihren Datenschutz, da diese Verordnung darauf abzielt, die Privatsphäre der Menschen im Internet zu schützen. Es gibt jedoch eine Menge Verhaltensweisen, die die Endbenutzer annehmen müssen, um ihre Rolle spielen zu können. Diese Verhaltensweisen sind allen Aktivitäten im Internet - von sozialen Medien bis hin zur Cloud - gemeinsam und werden gemeinhin als "die goldenen Regeln des Internets" bezeichnet.

Die erste Regel bezieht sich auf die Passwörter: **man muss eindeutige und starke Passwörter mit Zwei-Faktor-Authentifizierung haben**, während man sich einloggt und **sie alle drei Monate ändert**.
Die zweite Regel bezieht sich auf private Informationen: **Speichern oder teilen Sie keine sensiblen Informationen über das Internet**, insbesondere beim Online-Shopping; wenn Sie private Informationen in einem Cloud-Service gespeichert haben, achten Sie außerdem darauf**, dass Sie nicht alle Ihre Informationen in nur einer Wolke zusammenfassen!**

Die dritte Regel ist das Praktizieren von intelligentem Browsen: **Speichern Sie Ihre Anmeldedaten nicht** in einem Browser, einer Website oder Anwendung und melden Sie sich jedes Mal ab, wenn Sie eine Website verlassen. **Klicken Sie auch nicht** auf zweifelhafte Links oder geben Sie Ihre Daten nicht **auf ungesicherten Websites ein.**

Insgesamt müssen Sie anerkennen, dass es Ihre Daten sind, die schließlich durch Cyberangriffe kompromittiert werden könnten, und folglich müssen Sie sicherstellen, dass Sie Ihren Teil der Privatsphäre und der Datensicherheit im Internet einhalten.

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

Lösungsschlüssel
(die korrekten Antworten sind fett markiert)

1.Wissen anwenden

Situation: Was ist die Bedeutung von Cybersicherheit?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Cybersicherheit umfasst die Verteidigung von Hardware und Software.**
- **Cyberangriffe nehmen zu, und jeder ist heute anfälliger für diese Art von Vorfällen.**
- **Wirksame Cybersicherheitsmaßnahmen umfassen die Anwendung mehrerer Cybersicherheitsmaßnahmen.**
- **Aufgrund der Notwendigkeit der Anwendung mehrerer Cybersicherheitsmaßnahmen sollten so früh wie möglich Schulungen zur Cybersicherheit durchgeführt werden.**

2.Wissen anwenden

Situation: Bitte wählen Sie aus den folgenden Sätzen den richtigen aus.
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip: nur ein Satz ist wahr.

- Es wird empfohlen, ein einfaches Passwort zu wählen, um es sich besser merken zu können.
- Einige eindeutige Passwörter sind von einem Vornamen, dem Namen eines Familienmitglieds oder dem Namen eines Haustiers abgeleitet.
- Je mehr Zeichen und Symbole die Passwörter enthalten, desto weniger schwer sind sie zu erraten.
- **Ein sicheres Passwort besteht aus einer Kombination von Groß- und Kleinbuchstaben, Symbolen und Zahlen und ist mindestens acht Zeichen lang**.

Situation: Was sind einige der Regeln zum Schutz Ihrer digitalen Konten vor Cyberangriffen?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- Verwenden Sie dasselbe Passwort in mehreren Websites/Accounts.
- **Ändern Sie die Passwörter regelmäßig.**
- Speichern Sie die Anmeldedaten im Browser oder in der Anwendung eines bestimmten Computers.
- **Ein Fingerabdruck, ein Stimmabdruck oder ein Pincode sind eine gute Wahl für eine Zwei-Faktor-Authentifizierung.**
- **Vermeiden Sie beim Erstellen eines neuen Passworts Wörter aus dem Wörterbuch, Pronomen, Benutzernamen und andere vordefinierte Begriffe sowie häufig verwendete Passwörter.**

3.Wissen anwenden

Situation: Was sind einige der Informationen, die Sie beim Online-Shopping niemals angeben sollten?
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Sozialversicherungsnummer.**
- **Sicherheitscode der Kreditkarte.**
- **Nummer der Debitkarte.**

- **Bankkontonummer.**
- E-Mail-Adresse.

Situation: Bitte wählen Sie aus der Liste die richtigen Verhaltensweisen aus, um nicht Opfer von Cyberkriminalität zu werden
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Bevor die Kreditkarteninformationen angegeben werden, muss genügend Zeit für die Recherche auf der Website eingeplant werden.**
- **Kaufen Sie von einer Website, die über eine Verschlüsselung verfügt.**
- **Lesen Sie die Rückgabebestimmungen und andere Geschäftsbedingungen der Website sowie die Datenschutzrichtlinie der Website, bevor Sie etwas bestellen.**
- Bezahlen Sie mit einer Debitkarte, in bar oder per Überweisung.
- Verwenden Sie einen "Hotspot", um Ihre Vertraulichkeit zu schützen.

4.Wissen anwenden

Situation: Welche Aussage ist in Bezug auf Cloud Computing wahr?
Aufgabe: Wählen Sie die richtige Option nach dem Single-Choice-Prinzip: nur ein Satz ist wahr.

- Bei Platform as a Service (PaaS) bezahlt ein Unternehmen für Dienste wie Speicherung, Vernetzung und Virtualisierung nach dem Prinzip "Pay-as-the-go".
- Infrastructure as a Service (IaaS) ist ein Cloud-Computing-Modell, bei dem ein Drittanbieter Hardware- und Software-Tools bereitstellt Bankkontonummer
- **Software as a Service (SaaS) ist ein Software-Lizenzierungs- und Bereitstellungsmodell, bei dem Software auf Abonnementbasis lizenziert und zentral gehostet wird.**
- Bei der Nutzung von Cloud-Computern müssen Benutzer und Unternehmen physische Server verwalten.

Situation: Bitte wählen Sie aus der Liste die richtigen Verhaltensweisen aus, um nicht Opfer von Cyberkriminalität zu werden
Aufgabe: Wählen Sie die richtige(n) Option(en) nach dem Multiple-Choice-Prinzip aus: Keine, eine, mehr als eine oder alle Optionen können wahr sein.

- **Speichern Sie Informationen wie Adressen, Telefonnummern, Bankinformationen usw. in verschiedenen Wolken.**
- **Erstellen Sie ein eindeutiges Passwort nur für den Cloud-Service.**
- Bei der Verwendung von Cloud-Lösungen ist es nicht relevant, einen Virenschutz zu haben.
- Wegen seiner Bequemlichkeit wird empfohlen, die Anmeldedaten in der entsprechenden Anwendung zu speichern.