**Training Fiche**

|  |  |  |
| --- | --- | --- |
| **Titel** | Cybersicherheit und digitale Tools für KMU. Vorbereitet sein, um Cyber-Angriffe zu verhindern und zu lösen | |
| **Schlüsselwörter (meta tag)** | Cybersecurity, Sicherheit, Cyberkriminalität, Cyberangriff, | |
| **Zur Verfügung gestellt von** | ITSFA | |
| **Sprache** | Englisch | |
| **Bereich** | Digitale und Online-Kommunikation |  |
| Engagement des Teams und der Mitarbeiter von zu Hause aus |  |
| Vereinbarkeit von Berufs- und Privatleben |  |
| Selbst-Wohlbefinden |  |
| "Wie können Sie die Produktivität Ihres Teams von zu Hause aus steigern?" |  |
| Fernverwaltung von Projekten |  |
| Agiles Management nach Zielsetzungen |  |
| "Intelligente" Selbstwirksamkeit |  |
| Führung und Motivation in der Ära des intelligenten Arbeitens |  |
| Telearbeit: eine Auswahl digitaler Tools zur Verwaltung Ihres Unternehmens | **X** |
| **Zielsetzungen / Lernergebnisse** | | |
| In diesem Kurs erwerben Sie ein Grundwissen über Cybersicherheit, sowohl auf Unternehmensebene als auch auf der Ebene der Nutzer/Mitarbeiter. Sie lernen die Definitionen der wichtigsten Cyber-Risiken kennen, die Ihre Sicherheit und die Sicherheit Ihres Unternehmens gefährden können, und Sie lernen die wichtigsten Werkzeuge zur Verhinderung von Cyber-Verbrechen kennen, mit einem grundlegenden Leitfaden für Cybersicherheit, der Ihnen helfen wird, die grundlegenden Maßnahmen zu kennen, die Sie ergreifen müssen, um Ihr KMU vor diesen Bedrohungen zu schützen, und dann in der Lage zu sein, aus der Ferne auf sicherere Weise zu arbeiten | | |
| **Beschreibung** | | |
| Infolge der Covid-19-Pandemie sind die KMU aufgrund ihrer besonderen Merkmale zur Zielscheibe von Cyberkriminellen geworden. Die neuen Arbeitsformen, die durch die Pandemie entstanden sind, Telearbeit, also das so genannte "Smart Working", machen es erforderlich, dass die KMU Kenntnisse erwerben, die ihnen helfen, auf den Zug der Digitalisierung aufzuspringen und nicht zurückzubleiben. Einer der grundlegenden Ausbildungsbedürfnisse, die sich aus dieser Situation ergeben, ist die Cybersicherheit.  Mit diesem Kurs können sich die KMU ein Grundwissen über Cybersicherheit aneignen und verfügen somit über die Mittel, um in einer Welt, die sich ungebremst in Richtung Digitalisierung bewegt, Cyberrisiken zu vermeiden, die das Überleben ihrer Unternehmen gefährden. | | |
| **Inhalt in 3 Ebenen gegliedert** | | |
| 2. Cybersicherheit und digitale Werkzeuge für KMU. Vorbereitet sein, um Cyber-Angriffe zu verhindern und zu lösen  2.1 Sicherheit auf Unternehmensebene  -Was ist Cybersicherheit?  Aufgrund der Digitalisierung ist die Cybersicherheit für KMU heute ein wichtiges Thema. Cyberangriffe zielen zunehmend auf kleine und mittlere Unternehmen ab, die nicht so gut geschützt sind wie große Konzerne.  Cybersicherheit ist eine Reihe von Praktiken zum Schutz von Computersystemen und Software vor Cyberkriminalität. Cyberkriminalität ist jede kriminelle Aktivität, die in der digitalen Welt stattfindet, an der ein Computer, ein vernetztes Gerät oder ein Netzwerk beteiligt ist und die darauf abzielt, einen bestimmten Zweck oder Nutzen zu erreichen, der unterschiedlicher Art sein kann. Cybersicherheit umfasst viele Bereiche: Netzwerksicherheit, Anwendungssicherheit, Informationssicherheit, Benutzersicherheit usw. Sehen wir uns einige Konzepte an, um Cybersicherheit auf Unternehmensebene zu betrachten, damit wir am Ende des Kurses einen grundlegenden Leitfaden für Cybersicherheit haben.  -Ransomware  Ransomware ist eine Art von Schadsoftware, die Informationen auf verschiedenen Geräten verschlüsselt. Mit dieser Methode erpressen Cyberkriminelle Geld von ihren Opfern, indem sie ein Lösegeld für die Wiederherstellung des Zugangs zu ihren Daten verlangen.  Bei Ransomware handelt es sich um eine Art von Malware, die Benutzern den Zugriff auf ihr System oder ihre persönlichen Dateien verwehrt und die Zahlung eines Lösegelds verlangt, um den Zugriff darauf wiederherzustellen.  -Malware  Malware bedeutet bösartige Software. Malware ist eine der häufigsten Cyber-Bedrohungen und eine Software, die von Cyber-Kriminellen oder Hackern erstellt wurde, um den Computer eines rechtmäßigen Benutzers zu stören oder zu beschädigen. Malware wird oft über einen unaufgeforderten E-Mail-Anhang oder einen legitim aussehenden Download verbreitet und kann von Cyberkriminellen zum Geldverdienen oder für politisch motivierte Cyberangriffe verwendet werden. Es gibt viele verschiedene Arten von Malware, wie Viren, Trojaner, Spyware, Ransomware, Adware und Botnets.  -Antivirus  Ein Antivirus ist ein Programm, das Malware erkennt, sie blockiert und beseitigt, um eine Infektion des Geräts zu verhindern. Es gibt verschiedene Arten von Antivirenprogrammen. Um das für Sie oder Ihr Unternehmen am besten geeignete auszuwählen, müssen Sie die Spezifikationen des zu schützenden Geräts und einige zu berücksichtigende Kriterien in Betracht ziehen.  Es gibt eine Vielzahl von Antivirenprogrammen, daher sollten Sie bei der Auswahl diese Kriterien berücksichtigen:  -kompatibel mit Ihrem Betriebssystem  -Schutz Ihres Geräts, ohne dessen Geschwindigkeit, Kapazität oder Leistung zu beeinträchtigen.  -Häufige Aktualisierungen. Andernfalls könnten Sie neuen Bedrohungen ausgesetzt sein.  -Vielseitigkeit .Das Antivirus muss so vielseitig sein wie die Malware.  -Fähigkeit zu handeln. Es muss nicht nur die Bedrohung erkennen, sondern sie auch beseitigen und von unserem Gerät entfernen.  -Antimalware  Was ist der Unterschied zwischen Antivirus und Anti-Malware?  Beide Begriffe beziehen sich auf Software, die bösartige Software erkennen, schützen und entfernen soll. Entgegen dem, was der Name vermuten lässt, schützt Antiviren-Software vor mehr als nur Viren; sie verwendet einfach einen etwas altmodischen Namen, um zu beschreiben, was sie tut. Anti-Malware-Software dient ebenfalls dem Schutz vor Viren und verwendet einfach eine modernere Bezeichnung, die alle Arten von bösartiger Software, einschließlich Viren, umfasst.  Mit diesem Wissen kann Anti-Malware das Auftreten einer Virusinfektion verhindern und infizierte Dateien entfernen. Allerdings ist Anti-Malware nicht unbedingt in der Lage, Dateien wiederherzustellen, die ein Virus verändert oder ersetzt hat.  - Sicherheits-Patches. Schwachstelle  Sie ist ein wichtiger Bestandteil der Cybersicherheit in Unternehmen, da sie dazu beiträgt, Sicherheitslücken in den Systemen des Unternehmens zu vermeiden, indem alle Geräte und Anlagen aktualisiert werden. Dazu gehören Computeranwendungen und Betriebssysteme, Firmware für elektronische Geräte und Anti-Malware-Software. Patches und Updates werden von den eigentlichen Entwicklern der Software erstellt und dienen der Verbesserung ihrer Leistung durch Behebung von Sicherheitslücken und Hinzufügen neuer Funktionen.  - Schutz von Unternehmensdaten: Grundlagen der Datensicherung  Ganz einfach: Eine Datensicherung ist nichts anderes als eine Kopie der Dateien auf Ihrem Computer oder Gerät. Und wie die vielen oben beschriebenen Bedrohungen zeigen, ist eine Sicherung Ihrer wichtigen Unternehmensdateien und -daten aus einer Reihe wichtiger Gründe unerlässlich.  Jede Sicherung ist besser als keine Sicherung, aber nicht alle Sicherungsgeräte und -technologien sind gleich oder bieten das gleiche Maß an Schutz. Optimalen Schutz erhalten Sie, wenn Sie Ihre Daten nach der 3-2-1-Regel sichern, die wie folgt lautet  -Bewahren Sie mindestens drei (3) Kopien Ihrer Daten auf (so dass kein einzelnes Ereignis alle Kopien zerstört);  -Speicherung der Daten in mindestens zwei (2) verschiedenen Formaten (d. h. Festplatte, Band, Cloud usw.);  -Bewahren Sie eine (1) Kopie zum Schutz vor Feuer, Überschwemmung, Diebstahl und anderen physischen Katastrophen an einem anderen Ort auf.  Schutz von drahtlosen Netzwerken  Die Verwendung eines drahtlosen Netzwerks bietet Ihnen den Vorteil, dass Sie praktisch überall mit Ihrem Computer arbeiten und eine Verbindung zu anderen Computern im Netzwerk herstellen oder auf das Internet zugreifen können. Wenn Ihr drahtloses Netzwerk jedoch nicht sicher ist, bestehen erhebliche Risiken. Ein Hacker könnte zum Beispiel alle von Ihnen gesendeten oder empfangenen Daten abfangen, auf Ihre freigegebenen Dateien zugreifen, Ihre Internetverbindung kapern und Ihre Bandbreite oder Ihr Download-Limit ausschöpfen.  -Wenn Sie einen Wi-Fi-Router kaufen, hat er einen Standardnamen und ein Standardpasswort. Diese sind sehr leicht zu hacken, weshalb Sie sie ändern sollten. Darüber hinaus verfügt der Router über ein Administratorkennwort, mit dem Sie die Einstellungen des Routers ändern und verwalten können. Genau wie den Routernamen und das Passwort sollten Sie auch dieses Passwort ändern.  Um die Informationen zu schützen, die Sie über das Wi-Fi-Netzwerk senden, können Sie Ihr Netzwerk verschlüsseln, indem Sie die Software des Routers aktualisieren. Achten Sie auf die Einstellungen WPA3 oder WPA2, die die stärkste Verschlüsselung bieten.  Ausbildung der Mitarbeiter  Mitarbeiter können Ihr Unternehmen anfällig für Angriffe machen oder dazu beitragen, sie zu verhindern. Zahlreiche Studien zeigen, dass ein großer Teil der Datenverluste von internen Mitarbeitern verursacht wird, die in den meisten Fällen durch Unachtsamkeit oder Fehlinformationen Cyberkriminellen Zugang zu ihren Netzwerken gewähren.  Es gibt viele Szenarien, die zu Angriffen führen können, bei denen die Zugangswege Mitarbeiter sind. Zum Beispiel, wenn ein Mitarbeiter sein Arbeits-Tablet verliert, seine Anmeldedaten weitergibt oder betrügerische E-Mails öffnet, die Viren im Netzwerk verbreiten.  Um sich vor Insider-Bedrohungen zu schützen, ist es von entscheidender Bedeutung, in qualitativ hochwertige Cybersicherheitsschulungen für Mitarbeiter zu investieren, die ihnen das nötige Rüstzeug vermitteln, um in verschiedenen Situationen und bei verschiedenen Risiken handeln zu können.  Politiken. Cybersicherheitsrichtlinie. Was ist eine Cybersicherheitsrichtlinie?  Um Cyberkriminalität vorzubeugen, ist es nicht nur wichtig, Ihre Mitarbeiter in der Prävention von Cyberkriminalität zu schulen, sondern auch eine unternehmenseigene Cybersicherheitsrichtlinie zu erstellen. Darin werden die Richtlinien für die Übertragung von Unternehmensdaten, den Zugriff auf private Systeme und die Verwendung von Geräten, die das Unternehmen zur Verfügung stellt, klar umrissen. Achten Sie bei der Ausarbeitung Ihrer Richtlinie darauf, dass sie Ihren Mitarbeitern Anleitungen an die Hand gibt:   * die Art der Geschäftsinformationen, die weitergegeben werden können und wo * Zulässige Nutzung von Geräten und Online-Materialien * Umgang mit und Lagerung von sensiblem Material   Eine vollständige Vorlage für Cybersicherheitsrichtlinien umfasst die folgenden grundlegenden Teile:  -Einführung  -Zweck  -Umfang  -Vertrauliche Daten  Gerätesicherheit:  -Unternehmen Verwendung  -persönlicher Gebrauch  -E-Mail Sicherheit  -Übertragung von Daten  -Disziplinarmaßnahmen  2.2 Cybersicherheit auf Nutzer-/Mitarbeiterebene  Die Schulung von Endbenutzern ist wichtig, weil sie den unberechenbarsten Faktor der Cybersicherheit anspricht - den Menschen. Wenn gute Sicherheitsverfahren nicht befolgt werden, kann jeder versehentlich einen Virus in ein ansonsten sicheres System einschleusen. Den Benutzern beizubringen, auf Risikofaktoren zu achten, ist entscheidend für die Sicherheit eines jeden Unternehmens.  Schützen Sie die Daten auf Ihren Geräten  Personenbezogene Daten und sensible Daten. Sind sie dasselbe?  Was sind personenbezogene Daten?  Personenbezogene Daten sind alle Informationen, anhand derer eine lebende Person mit einem gewissen Grad an Genauigkeit identifiziert werden kann. So gilt beispielsweise die E-Mail-Adresse eines Mitarbeiters eines Unternehmens als personenbezogene Daten, da sie angibt, dass diese Person für das Unternehmen arbeitet. Eine physische Adresse oder eine Telefonnummer sind ebenfalls personenbezogene Daten, da diese Informationen dazu verwendet werden können, die Person zu kontaktieren.  Alles, was Ihre physische Anwesenheit an einem Ort bestätigen kann, gilt ebenfalls als personenbezogene Daten. Zum Beispiel sind Aufnahmen von Überwachungskameras personenbezogene Daten, ebenso wie Fingerabdrücke.  Einige Beispiele könnten sein:  -Vorname und Nachname  -Wohnadresse  -Eine E-Mail Adresse  -Eine Personalausweisnummer  -Standortdaten  Eine Internet-Protokoll-Adresse (IP)  -Die Werbekennung Ihres Telefons  Was sind sensible personenbezogene Daten?  Bei sensiblen personenbezogenen Daten handelt es sich um eine spezifische Gruppe von "besonderen Kategorien", die einen stärkeren gesetzlichen Schutz genießen und mit besonderer Sicherheit behandelt werden müssen, wenn die Person, auf die sich diese Daten beziehen, ausdrücklich zustimmt. Dazu gehören Informationen, die sich auf Folgendes beziehen:  -Rassische oder ethnische Herkunft;  -Politische Meinungen;  -Religiöse oder philosophische Überzeugungen;  -Mitgliedschaft in einer Gewerkschaft;  -Genetische Daten; und  -Biometrische Daten (wenn sie zur eindeutigen Identifizierung einer Person verarbeitet werden).  Sensible personenbezogene Daten sollten getrennt von anderen personenbezogenen Daten aufbewahrt werden, vorzugsweise in einer verschlossenen Schublade oder einem Aktenschrank. Wie bei personenbezogenen Daten im Allgemeinen sollten sie nur dann auf Laptops oder Handheld-Geräten gespeichert werden, wenn die Datei verschlüsselt und/oder pseudonymisiert wurde.  Physische Sicherheit  Cybersicherheit beginnt mit starker physischer Sicherheit. Dazu gehört, dass Dokumente sicher aufbewahrt werden, dass sie in einem Raum oder Schrank eingeschlossen werden, dass der physische Zugang zu sensiblen Daten eingeschränkt wird, dass Informationen korrekt gelöscht werden und dass Dokumente mit sensiblen Daten geschreddert werden, wenn sie nicht mehr benötigt werden. Erlauben Sie den Zugang zu persönlichen und finanziellen Informationen nur den Mitarbeitern, die sie wirklich benötigen.  -Erinnern Sie Ihre Mitarbeiter daran, sensible Daten niemals unbeaufsichtigt am Arbeitsplatz oder an öffentlichen Orten liegen zu lassen. Versäumnisse bei der physischen Sicherheit können dazu führen, dass sensible Unternehmensdaten dem Identitätsdiebstahl zum Opfer fallen, was schwerwiegende Folgen haben kann.  Sie alle können durch physische Sicherheitsverletzungen entstehen, z. B. durch den Verlust eines Laptops, den Diebstahl eines Mobiltelefons oder das Verlegen eines Flash-Laufwerks. Wenn die Informationen auf diesen Geräten geschützt sind, ist es weniger wahrscheinlich, dass sie zu einer Datenschutzverletzung führen.  Hier sind einige nützliche Beispiele:  Verlangen Sie komplexe Passwörter: Verlangen Sie lange, komplexe und eindeutige Passwörter. Und stellen Sie sicher, dass diese Passwörter sicher gespeichert werden. Erwägen Sie die Verwendung eines Passwortmanagers.  Verwenden Sie eine Multi-Faktor-Authentifizierung: Verlangen Sie eine Multi-Faktor-Authentifizierung für den Zugriff auf Bereiche Ihres Netzwerks mit sensiblen Informationen. Dies erfordert zusätzliche Schritte über die Anmeldung mit einem Passwort hinaus, beispielsweise einen temporären Code auf einem Smartphone.  Anmeldeversuche begrenzen: Begrenzen Sie die Anzahl der fehlerhaften Anmeldeversuche, die zum Entsperren der Geräte erlaubt sind. Dies trägt zum Schutz vor Eindringlingen bei.  Verschlüsseln: Verschlüsseln Sie tragbare Geräte, einschließlich Laptops und USB-Sticks, die sensible Daten enthalten. Verschlüsseln Sie alle sensiblen Daten, die Sie außerhalb des Unternehmens versenden, z. B. an einen Buchhalter oder Anwalt.  -E-Mail-Sicherheit  Für den Fall, dass der Nutzer/Mitarbeiter persönliche Geräte für den Zugriff auf die Systeme des Unternehmens oder für den persönlichen Gebrauch verwendet, sollten bestimmte Sicherheitsmaßnahmen in Bezug auf die Nutzung von E-Mail getroffen werden, da dies auch ein Einfallstor für kriminelle Handlungen sein kann. Falls Mitarbeiter ihre persönlichen Geräte für den Zugriff auf die Systeme des Unternehmens verwenden müssen, sollten sie diese Informationen der Geschäftsleitung zur Protokollierung melden.  Um den Schutz der Unternehmenssysteme zu gewährleisten, sollten alle Mitarbeiter:  -Stellen Sie sicher, dass alle persönlichen Geräte, die für den Zugang zu den Systemen des Unternehmens verwendet werden, mit einem Passwort geschützt sind (mindestens 8 Zeichen).  -Installieren Sie eine umfassende Antiviren-Software.  -Regelmäßige Aktualisierung der Antiviren-Software.  -Sperren Sie alle Geräte, wenn sie unbeaufsichtigt sind.  -Stellen Sie sicher, dass alle Geräte jederzeit geschützt sind.  -Verwenden Sie stets sichere, private Netze.  Der Schutz von E-Mail-Systemen hat hohe Priorität, da E-Mails zu Datendiebstahl und Betrug führen und bösartige Software wie Würmer und Bugs enthalten können. Daher wird den Nutzern/Mitarbeitern empfohlen,:  Überprüfen Sie die Legitimität jeder E-Mail, einschließlich der E-Mail-Adresse und des Namens des Absenders.  -Vermeiden Sie es, verdächtige E-Mails und Anhänge zu öffnen und auf Links zu klicken.  -Achten Sie auf signifikante grammatikalische Fehler.  -Vermeiden Sie Titel und Links, die zum Klicken verleiten.  Kontaktieren Sie die IT-Abteilung, wenn Sie verdächtige E-Mails erhalten haben.  Phishing  Auch bekannt als elektronischer Betrug. Wenn wir ein wenig mehr über die häufigsten und gefährlichsten Betrugsfälle wissen, können wir vermeiden, ihnen zu verfallen.  Mit diesen Methoden, "Phishing" und "Smishing", versucht der Angreifer, an private Informationen wie Passwörter oder Kreditkarten zu gelangen. Bei diesem Angriff wird das Opfer per E-Mail um gefährdete Daten wie Passwörter oder Zugangscodes gebeten, wobei er vorgibt, die legitime Website oder Einrichtung zu sein, damit das Opfer die vom Angreifer angeforderten Daten übermittelt.  Smishing  Diese Bedrohung ähnelt dem Phishing, mit dem einzigen Unterschied, dass sie per SMS an Telefone gesendet wird. Der Hacker sendet eine Nachricht an unsere Telefone, das Öffnen der Nachricht ist nicht gefährlich. Die Gefahr besteht darin, auf den Link zu klicken, denn dann beginnt der Angriff.  2. 3 Die häufigsten Cyberrisiken, die man kennen sollte. Der grundlegende Leitfaden für Cybersecurity  Nachdem wir uns mit den oben erwähnten Konzepten vertraut gemacht haben, wollen wir einen Blick auf die häufigsten Risiken werfen, mit denen KMU konfrontiert sind. Dies geht aus Studien hervor, die auf der Erhebung der Europäischen Agentur für Cybersicherheit (ENISA) basieren, wobei Phishing- und webbasierte Angriffe die Liste anführen.  1) Phishing-Angriffe  Diese Art von Angriffen ist aufgrund der Fernarbeit sehr beliebt geworden. Ein unvorsichtiger Klick auf einen Link genügt einem Cyberkriminellen, um Zugang zu sensiblen Geschäftsdaten zu erhalten.  2) Webbasierte Angriffe  Cyberkriminelle nutzen fast jede Schwachstelle - innerhalb eines Betriebssystems oder einer Anwendung - für einen Angriff. Die meisten Cyberkriminellen entwickeln jedoch Web-Bedrohungen, die gezielt auf einige der gängigsten Betriebssysteme und Anwendungen abzielen  3) Allgemeine Malware-Angriffe  Viele KMU unterschätzen aufgrund ihrer Größe die Möglichkeit von Cyberangriffen. Doch genau darauf haben es Hacker abgesehen, denn sie können schnell von einer Ransomware-Bedrohung für weniger sichere KMU profitieren.  4) Böswillige Insider  Diese Art der Bedrohung bezieht sich auf das Vorhandensein von Personen innerhalb einer Organisation (u.a. interne Mitarbeiter oder externe Zulieferer), die aus Unachtsamkeit, Unwissenheit und/oder Bösgläubigkeit eine "Aktion" durchführen, die die Sicherheit von Prozessen, Systemen oder Einrichtungen einer industriellen Betriebsumgebung oder kritischen Infrastruktur beeinträchtigt.  5) Denial-of-Service-Angriffe  Ziel dieser Angriffe ist es, die Website eines Unternehmens so zu stören, dass sie nicht mehr zugänglich ist, was von den Cyberkriminellen aus verschiedenen Gründen getan wird. Eine gestoppte Website kann zu Umsatzeinbußen, Datenverstößen, Misstrauen der Kunden und einer Lähmung der Unternehmenstätigkeit führen.  Der grundlegende Leitfaden zur Cybersicherheit  1. Ermitteln Sie Ihre Schwachstellen  Als Erstes müssen Sie Ihre Schwachstellen ermitteln, damit Sie wissen, welche Daten Sie schützen müssen. Stellen Sie sich Fragen wie: Welches sind die wichtigsten Daten, die mein Unternehmen speichert? Wo werden diese Daten gespeichert?  Sobald Sie die Antworten kennen, können Sie mit der Bewertung der Risiken beginnen.  2. Schützen Sie Ihre Geräte  Arbeitsgeräte sind entscheidend für die Leistung Ihres Unternehmens. Ihre Internetverbindung macht sie anfällig für Cyberangriffe. Hier sind einige Tipps zum Schutz dieser Geräte  A. Aktualisieren Sie Ihre Software  B. Schützen Sie sich vor Viren  C. Einrichten einer Firewall  D. Besondere Vorsichtsmaßnahmen für Laptops und andere mobile Geräte  3. Schützen Sie Ihre Daten  Unabhängig davon, in welcher Art von Unternehmen Sie tätig sind, sind Daten ein wesentlicher Bestandteil davon. Daten können auf tausend verschiedene Arten beschädigt werden, eine davon sind Cyberangriffe. Hier sind einige nützliche Tipps, wie Sie Ihre Daten schützen können.  A. Einführung eines Verfahrens zur Sicherung kritischer Daten  B. Verschlüsseln Sie vertrauliche Unternehmensdaten, die Sie in der Cloud speichern  C. Schützen Sie Ihre Passwörter  D. Berechtigungen festlegen  E. Schützen Sie Ihre drahtlosen Netzwerke  F. Sicheres Surfen im Internet  G. Schutz vertraulicher Informationen, die von Fernarbeitern erstellt werden  H. Schützen Sie Ihre Kundendaten  4. Verankerung der Cybersicherheit am Arbeitsplatz  Die in diesem grundlegenden Leitfaden genannten Sicherheitsmaßnahmen können Ihnen helfen, das Risiko eines Cyberangriffs erheblich zu verringern. Dies nützt jedoch nichts, wenn die Mitarbeiter Ihres Unternehmens nicht über das nötige Bewusstsein und die nötige Ausbildung verfügen, um zur Prävention beitragen zu können. Nehmen Sie diese Art von Schulung in Ihr Unternehmen auf, und vergessen Sie nicht, eine unternehmenseigene Cybersicherheitsrichtlinie zu erstellen, die alle Teammitglieder befolgen können. | | |
| **Inhalt in Aufzählungspunkten** | | |
| 2. Cybersicherheit und digitale Werkzeuge für KMU. Vorbereitet sein, um Cyber-Angriffe zu verhindern und zu lösen  2.1 Sicherheit auf Unternehmensebene  2.2 Cybersicherheit auf Nutzer-/Mitarbeiterebene  2.3 Die häufigsten Cyber-Risiken, die es zu beachten gilt. Der grundlegende Leitfaden für Cybersicherheit | | |
| **5 Glossareinträge** | | |
| Cybersicherheit: Ist eine Reihe von Praktiken zum Schutz von Computersystemen und Software vor Cyberkriminalität. Cybersicherheit umfasst viele Bereiche: Netzsicherheit, Anwendungssicherheit, Informationssicherheit, Benutzersicherheit usw.  Cyberkriminalität: Jede kriminelle Aktivität, die in der digitalen Welt stattfindet, an der ein Computer, ein vernetztes Gerät oder ein Netzwerk beteiligt ist und mit der ein bestimmter Zweck oder Nutzen erreicht werden soll, der unterschiedlicher Art sein kann. **5 Glossareinträge**  Ransomware: Ist eine Art von Schadsoftware, die Informationen auf verschiedenen Geräten verschlüsselt. Mit dieser Methode erpressen Cyberkriminelle Geld von ihren Opfern, indem sie ein Lösegeld für die Wiederherstellung des Zugangs zu ihren Daten verlangen.  Malware: Das bedeutet bösartige Software. Malware ist eine der häufigsten Cyber-Bedrohungen. Sie ist eine Software, die von Cyber-Kriminellen oder Hackern erstellt wurde, um den Computer eines rechtmäßigen Benutzers zu stören oder zu beschädigen. Es gibt viele verschiedene Arten von Malware, wie: Viren, Trojaner, Spyware, Ransomware, Adware, Botnets.  Sicherung: Ganz einfach: Eine Datensicherung ist nichts anderes als eine Kopie der Dateien auf Ihrem Computer oder Gerät. Und wie die vielen oben beschriebenen Bedrohungen zeigen, ist eine Sicherung Ihrer wichtigen Geschäftsdateien und -daten aus einer Reihe wichtiger Gründe unerlässlich.**äge** | | |
| **Bibliographie und weitere Referenzen** | | |
| <https://atlasvpn.com/blog/phishing-and-web-based-attacks-were-the-most-common-among-europes-smes>  <https://www.kaspersky.com/resource-center/preemptive-safety/protecting-wireless-networks>  <https://www.pandasecurity.com/es/mediacenter/seguridad/parches-brechas-datos/>  <https://searchsecurity.techtarget.com/definition/cybercrime>  <https://es.malwarebytes.com/antivirus/>  <https://ciberseguridad.com/normativa/espana/medidas/actualizaciones/>  <https://www.betterteam.com/cyber-security-policy>  <https://business.gov.au/online/cyber-security/create-a-cyber-security-policy>  <https://www.daemon4.com/empresa/noticias/las-principales-amenazas-de-ciberseguridad-para-pymes/>  <https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data>  <https://www.bbva.com/es/phishing-y-smishing-que-son-y-como-evitarlos/>  <https://www.ciberseguridadlogitek.com/la-amenaza-del-malicious-insider-en-los-entornos-de-operacion-industrial-y-de-infraestructuras-criticas/>  <https://usa.kaspersky.com/resource-center/threats/web>  <https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/>  <https://es.vpnmentor.com/blog/la-guia-completa-de-ciberseguridad-para-pequenas-y-medianas-empresas/>  <https://www.ncsc.gov.uk/collection/small-business-guide>  <https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf>  <https://www.kaspersky.com/resource-center/preemptive-safety/small-business-cyber-security>  <https://ciberseguridadbidaidea.com/ciberseguridad/6-principales-amenazas-de-una-empresa-en-ciberseguridad/>  <https://www.widefense.com/recursos/ciberseguridad/pequenas-empresas/>  <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>  <https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-choices>  <https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware>  <https://internetpasoapaso.com/antimalware/>  <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited>  <https://me-en.kaspersky.com/blog/how-to-set-up-wifi-router/4390/>  <https://blog.walkme.com/5-employee-training-fails/>  <https://almamate.in/importance-of-selecting-the-best-salesforce-institute-in-noida/>  <https://cmitsolutions.com/blog/6-ways-protect-data-devices-digital-identity/>  <http://www.rbntechnologies.com/products.html>  <https://memoori.com/physicalsecurity-2016-rounded_v1/>  <https://www.djcs.com.ve/djcsnews/1901-automationedge-password-reset>  <https://www.datacenterknowledge.com/security/managing-encryption-data-centers-hard-and-it-will-get-harder>  <https://nakedsecurity.sophos.com/es/2016/08/09/email-how-secure-is-yours-survey/>  <https://www.valoradata.com/blog/que-es-el-phishing/>  <https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/>  <https://www.keepnetlabs.com/7-ways-to-prevent-phishing-attacks-in-2021/>  <https://www.teceze.com/what-is-vmdr-vulnerability-management>  <https://cypheradda.blogspot.com/2019/05/5-cybersecurity-tips-for-workplace.html>  <https://molinaoposiciones.com/2021/03/22/por-fin-fecha-definitiva-de-auxilio/>  <https://unaaldia.hispasec.com/2021/04/malware-en-plantillas-empresariales-de-descarga-gratuita.html> | | |
| **5 Multiple-Choice-Fragen zur Selbsteinschätzung** | | |
| 1) Was sind personenbezogene Daten?  **a) Personenbezogene Daten sind alle Informationen, anhand derer eine lebende Person mit einem gewissen Grad an Genauigkeit identifiziert werden kann. So gilt beispielsweise die E-Mail-Adresse eines Mitarbeiters eines Unternehmens als personenbezogene Daten, da sie angibt, dass diese Person für das Unternehmen arbeitet.**  b) Personenbezogene Daten sind eine spezifische Gruppe von "besonderen Kategorien", die einen stärkeren gesetzlichen Schutz genießen und mit besonderer Sicherheit behandelt werden müssen, wenn die Person, auf die sich diese Daten beziehen, ausdrücklich zustimmt.  2) Wählen Sie die richtige Antwort im Zusammenhang mit dem Konzept der Sicherheits-Patches.  **a) Sie ist ein wichtiger Bestandteil der Cybersicherheit in Unternehmen, da sie dazu beiträgt, Sicherheitslücken in den Systemen des Unternehmens zu vermeiden, indem alle Geräte und Anlagen aktualisiert werden. Dazu gehören Computeranwendungen und Betriebssysteme, Firmware für elektronische Geräte und Anti-Malware-Software.**  b) Es ist ein wichtiger Teil der Cybersicherheit, der die sichere Aufbewahrung von Dokumenten, das Abschließen in einem Raum oder Schrank, die Beschränkung des physischen Zugangs zu sensiblen Daten, das korrekte Löschen von Informationen und das Schreddern von Dokumenten mit sensiblen Daten, wenn sie nicht mehr benötigt werden, umfasst.  3) Warum ist eine Endbenutzerschulung im Hinblick auf die Cybersicherheit auf Benutzerebene wichtig?  a) Es ist nicht so wichtig, da der Endnutzer der einzige ist, der von der Cyberkriminalität betroffen ist und keine andere Wahl hat, als ein gutes Virenschutzprogramm zu installieren.  b) **Die Schulung von Endbenutzern ist wichtig, weil sie den unberechenbarsten Faktor der Cybersicherheit anspricht - den Menschen.**  4) Was ist der Unterschied zwischen Antivirus und Anti-Malware?  a) Sie beziehen sich beide auf Software, die bösartige Software erkennen, schützen und entfernen soll.  b) Nur ein Anti-Malware-Programm kann bösartige Software aufspüren, ein Antivirus Programm ist speziell darauf ausgelegt, die Bedrohung vom Computer zu entfernen.    5) Wählen Sie die richtige Option zum Schutz von drahtlosen Netzwerken.  **a) Wenn Ihr drahtloses Netzwerk nicht sicher ist, besteht ein erhebliches Risiko. Ein Hacker könnte zum Beispiel alle von Ihnen gesendeten oder empfangenen Daten abfangen, auf Ihre freigegebenen Dateien zugreifen, Ihre Internetverbindung kapern und Ihre Bandbreite oder Ihr Download-Limit ausschöpfen.**  **b) Wenn Sie einen Wi-Fi-Router kaufen, hat er einen Standardnamen und ein Standardpasswort. Diese sind sehr leicht zu hacken, also sollten Sie sie ändern. Außerdem verfügt der Router über ein Administrator-Passwort, mit dem Sie die Einstellungen des Routers ändern und verwalten können; auch dieses Passwort sollten Sie ändern.** | | |
| **Verwandtes Material** |  | |
| **Verwandte PPT** | SWIFTSME\_Kurs 2\_Cybersecurity und digitale Tools für KMU. Vorbereitet sein, um Cyber-Angriffe zu verhindern und zu lösen\_DE | |
| **Referenz-Link** |  | |
| **Video im YouTube-Format (falls vorhanden)** |  | |