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

InCyT-Trainingsmodule

Informationssicherheit für Manager Einheit 3 - Wochen 5 Name der Einheit (des Moduls): Management der Informationssicherheit 3	
Lernaktivitäten	❑ **Webinar**❑ **Übungen**❑ **Workshop**❑ **Präsentation**❑ **Sonstiges**
Lehrverantwortliche	• George Matache et al.
Ziele der Lernaktivitäten	1 Allgemeine Terminologie 2. Vertraulichkeit, Integrität und Verfügbarkeit (CIA) 3. Regeln und Normen 4. Management der Informationssicherheit 5. Wie funktioniert die Malware? 6. Die größten Cyber-Bedrohungen 7. Arten von Angriffen 8. Sicherer Webserver - SSL 9. Versenden und Empfangen von E-Mails 10. Vermögensverwaltung
Zu erwerbende Fertigkeiten	-TS3 Netzwerksicherheit -TS4 Penetrationstests (ausnutzbare Schwachstellen) - SS3 Kognitions- und Verhaltensanalyse
Dauer der Lernaktivität	2 Wochen
Lernanforderungen	***Was wird benötigt?***
	• Zugang zum Internet • Internet-Browser • MS Büro365

Kurze Informationen über das Modul

Beschreibung
Cybersicherheit ist die Praxis des Schutzes von Computern, Servern, mobilen Geräten, elektronischen Systemen, Netzwerken und Daten vor bösartigen Angriffen. Sie wird auch als Sicherheit der Informationstechnologie oder elektronische Informationssicherheit bezeichnet. Der Begriff findet in einer Vielzahl von Kontexten Anwendung, von Unternehmen bis hin zu mobilen Computern, und kann in einige allgemeine Kategorien unterteilt werden. Unternehmen sind oft so sehr mit ihrem Tagesgeschäft beschäftigt, dass sie vergessen, in die Netzsicherheit zu investieren. Andere sind sich der Notwendigkeit einer umfassenden Netzwerksicherheit bewusst, verfolgen aber eine nachsichtige Strategie in Bezug auf ihre IT, was sich im Falle eines Datenlecks als ebenso nachteilig erweisen kann. Um Ihre Daten und letztlich Ihr Unternehmen zu schützen, müssen Sie wissen, was Netzwerksicherheit bedeutet und welche bewährten Verfahren Sie anwenden können, um das Netzwerk Ihres Unternehmens vor den zahlreichen Bedrohungen von außen zu schützen, die versuchen, in Ihr Netzwerk einzudringen. Es ist äußerst wichtig, dass die Schulung zum Thema Cybersicherheit für KMU - Manager und Mitarbeiter - konkret und interaktiv ist und auch praxisnah, da die kleinen KMU weder Zeit, Motivation noch Ressourcen haben, um sich mit diesem Thema zu befassen, weshalb es sehr wichtig ist, dass die Schulung für die teilnehmenden Manager relevant und handhabbar ist. Daher ist dieses Modul auf dieser Grundlage geplant. Das Informationssicherheitsmanagement (ISM) definiert und verwaltet die Kontrollen, die eine Organisation einführen muss, um sicherzustellen, dass sie die Vertraulichkeit, Verfügbarkeit und Integrität von Ressourcen vor Bedrohungen und Schwachstellen sinnvoll schützt. Malware oder "bösartige Software" ist ein Oberbegriff, der jedes bösartige Programm oder jeden bösartigen Code beschreibt, der für Systeme schädlich ist. Malware ist feindselig, aufdringlich und absichtlich bösartig. Sie versucht, in Computer, Computersysteme, Netzwerke, Tablets und mobile Geräte einzudringen, sie zu beschädigen oder zu deaktivieren, indem sie häufig die teilweise Kontrolle über den Betrieb eines Geräts übernimmt. Wie die menschliche Grippe stört sie das normale Funktionieren. Die Motive für Malware sind unterschiedlich. Malware kann darauf abzielen, mit Ihnen Geld zu verdienen, Ihre Arbeit zu sabotieren, ein politisches Statement abzugeben oder einfach nur damit zu prahlen. Obwohl Malware die physische Hardware von Systemen oder Netzwerkgeräten nicht beschädigen kann, kann sie Ihre Daten stehlen, verschlüsseln oder löschen, zentrale Computerfunktionen verändern oder kapern und Ihre Computeraktivitäten ohne Ihr Wissen oder Ihre Zustimmung ausspionieren. Malware wird beschrieben und definiert, ihre vielen verschiedenen Arten werden vorgestellt und ihre Funktionsweise erklärt. Wir beschreiben auch die Warnzeichen eines infizierten Geräts und erklären, wie man sich davor schützen kann. Die Lernenden können über diese Aspekte informiert

werden, indem sie den entsprechenden Text lesen, sich Streaming-Webinare ansehen und Übungen im eigenen Tempo und durch Live-Interaktion mit dem Publikum mit kontinuierlichem Feedback und Gamification-Wissenscheck lösen.

Inhalt des Lernmaterials

Vor allem, wenn Sie ein Unternehmen haben, das sehr stark davon abhängig ist, dass Ihre IT-Systeme funktionieren und sicher sind. Die Bedrohungen für die Cybersicherheit nehmen immer mehr zu.

Cyberangriffe haben in der EU in den Jahren 2020 und 2021 und vor allem 2022 weiter zugenommen, und zwar sowohl in Bezug auf ihre Raffinesse und Anzahl als auch in Bezug auf ihre Auswirkungen. Die EU arbeitet an mehreren Fronten, um Bürger und Unternehmen vor Cyberkriminalität zu schützen und einen sicheren, offenen und geschützten Cyberraum zu gewährleisten.

Im Jahr 2022 werden staatlich geförderte Gruppen die Kryptowährungsbranche ins Visier nehmen, während Cyberkriminelle Investoren ausnutzen werden, indem sie digitale Geldbörsen mit eingebauten Hintertüren entwickeln. Wir werden wahrscheinlich eine Zunahme der Angriffe auf Zahlungssysteme und fortschrittlichere mobile Bedrohungen erleben.

Ungefähr die Hälfte (47 %) der dänischen Bevölkerung zwischen 16 und 89 Jahren hat schon einmal mit Internetkriminalität in Form von gefälschten E-Mails, Betrug, Hacking oder Identitätsdiebstahl zu tun gehabt. Das Gleiche gilt für 11 Prozent der dänischen Privatunternehmen. 8 Prozent der Unternehmen haben erlebt, dass der Zugang zu digitalen Diensten blockiert wurde, und bei 3 Prozent wurden Daten gelöscht oder zerstört. Phishing ist das am weitesten verbreitete Problem, aber leider sehen wir auch einen radikalen Anstieg der Zahl gefälschter Websites, da immer mehr Menschen von zu Hause aus einkaufen und arbeiten.

Das Kernstück des ISM ist das Informationsrisikomanagement, ein Prozess, der die Bewertung der Risiken, mit denen eine Organisation bei der Verwaltung und dem Schutz von Vermögenswerten umgehen muss, sowie die Weitergabe der Risiken an alle geeigneten Interessengruppen umfasst. Dies erfordert eine ordnungsgemäße Identifizierung und Bewertung der Vermögenswerte, einschließlich der Bewertung des Wertes der Vertraulichkeit, Integrität, Verfügbarkeit und des Ersatzes der Vermögenswerte. Als Teil des Informationssicherheitsmanagements kann eine

Organisation ein Managementsystem für Informationssicherheit und andere bewährte Verfahren einführen, die in den Normen ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27035 zur Informationssicherheit enthalten sind. Diese Art der Zertifizierung ist jedoch oft zu ressourcenintensiv für KMU, weshalb wir uns auf eine agile Cybersicherheitspraxis vorbereiten:

Informationssicherheit und interne Kontrollsysteme

- Allgemeine Terminologie
- CIA-Trias
- Anatomie eines Angriffs (Reduzierung der Angriffsfläche)
- Rahmenwerke für Cybersicherheit

Management der Informationssicherheit
E-Mail & Büro
Geräte
Eine der größten Herausforderungen für KMU ist Malware, ein Oberbegriff für jede Art von "bösartiger Software", die darauf ausgelegt ist, ohne Ihr Wissen in Ihr Gerät einzudringen. Es gibt viele Arten von Malware, und jede arbeitet anders, um ihre Ziele zu erreichen. Alle Malware-Varianten haben jedoch zwei entscheidende Merkmale gemeinsam: Sie sind heimtückisch und arbeiten aktiv gegen Ihre Interessen.

Ist Malware ein Virus? Ja und nein. Während alle Computerviren Malware sind, sind nicht alle Malwares Viren. Viren sind nur eine Art von Malware. Viele Leute verwenden diese beiden Begriffe synonym, aber aus technischer Sicht sind Viren und Malware nicht dasselbe.
Betrachten Sie es einmal so: Malware ist bösartiger Code. Computerviren sind bösartiger Code, der sich über Computer und Netzwerke verbreitet.

Wie funktioniert die Malware?

Alle Schadprogramme folgen demselben Grundmuster: Der Benutzer lädt die Malware unwissentlich herunter oder installiert sie, wodurch das Gerät infiziert wird.

Die meisten Malware-Infektionen treten auf, wenn Sie versehentlich eine Aktion ausführen, durch die die Malware heruntergeladen wird. Diese Aktion kann das Anklicken eines Links in einer E-Mail oder der Besuch einer bösartigen Website sein. In anderen Fällen verbreiten Hacker Malware über Peer-to-Peer-Filesharing-Dienste und kostenlose Softwarepakete. Das Einbetten von Malware in einen beliebten Torrent oder einen Download ist ein effektiver Weg, um sie über eine breite Benutzerbasis zu verbreiten. Mobile Geräte können auch über Textnachrichten infiziert werden.

Eine andere Technik besteht darin, Malware in die Firmware eines USB-Sticks oder Flash-Laufwerks zu laden. Da die Malware auf die interne Hardware des Geräts geladen wird (und nicht auf den Dateispeicher), ist es unwahrscheinlich, dass Ihr Gerät die Malware erkennt. Aus diesem Grund sollten Sie niemals ein unbekanntes USB-Laufwerk an Ihren Computer anschließen.

Sobald die Malware installiert ist, infiziert sie Ihr Gerät und beginnt, die Ziele der Hacker zu erreichen. Was die verschiedenen Arten von Malware voneinander unterscheidet, ist die Art und Weise, wie sie dies tun. Wie also funktioniert Malware? Was ist ein Malware-Angriff?

Die größten Cyber-Bedrohungen

Drive-by-Exploits können automatisch vorhandene Schwachstellen in der auf einem PC installierten Software ausnutzen, ohne mit dem rechtmäßigen Benutzer zu interagieren; 2012 wurde ihr Anwendungsbereich auch auf mobile Endgeräte ausgeweitet. Sie konzentrieren sich fast ausschließlich auf die Kompromittierung rechtmäßiger Websites. Schwachstellen im Browser, seinen Plugins oder dem Betriebssystem können ausgenutzt werden, um Malware ohne das Wissen des Benutzers auf dem PC zu installieren.
Würmer sind selbstreplizierende Programme, die das Computernetz nutzen, um ihre eigenen Kopien an andere Knoten (Computer im Netz) zu senden, und zwar ohne das Eingreifen eines Benutzers. Im Gegensatz zu einem Computervirus muss ein Computerwurm nicht an ein bestehendes Programm angehängt werden, sondern er schädigt das Netz, indem er einfach nur Bandbreite beansprucht.

Trojaner präsentieren sich in Form legitimer Programme, die in Wirklichkeit mit dem Ziel erstellt werden, vertrauliche Daten zu stehlen oder unbefugten Benutzern oder Programmen den Zugriff auf das infizierte System zu ermöglichen; sie machen die große Mehrheit der Infektionen aus (80 %).

Malware ist jedes Programm, dessen Funktion darin besteht, Software- oder Hardwareschäden an einem Computer zu verursachen (z. B. Viren) - wie oben beschrieben.

Viren zielen darauf ab, so viele PCs wie möglich zu infizieren, während Spyware darauf abzielt, sich über das Internet zu verbreiten. Viren haben in der Regel eine gefährliche Nutzlast, sie wollen dem infizierten Computer Schaden zufügen, während Spyware nur die Computerprozesse verlangsamt, Popups hinzufügt, den Browser destabilisiert und andere "lästige" Effekte hat.

SQL-Injektion (Code-Injektion) liegt vor, wenn ein Angreifer beliebige Daten in eine an eine Datenbank gesendete SQL-Abfrage einfügen kann; durch Injektion der Syntax wird die Logik der

Anweisung so verändert, dass sie eine andere Aktion ausführt; dies ist die häufigste Sicherheitslücke. Die beste Strategie zur Abwehr von SQL-Injektionen besteht darin, starke Eingabevalidierungsroutinen zu implementieren, damit der Angreifer keine Daten eingeben kann, die nicht für die Anwendung erforderlich sind.

Spyware wird im Allgemeinen als ein Programm definiert, das die Schwachstellen eines Systems zum Vorteil eines Dritten ausnutzt. Es kann Ihren Computer verlangsamen, ihn anfällig für Vireninfektionen machen und vertrauliche Informationen wie Benutzernamen für verschiedene Anwendungen, Passwörter und Kreditkarten-/Bankkontodaten sammeln.

Ein Keylogger ist ein kleines "intelligentes" Programm, das Hacker auf Ihrem Computer platzieren, ohne dass Sie es merken. Dort kann es mehrere Monate oder Jahre lang liegen und jeden einzelnen Tastendruck, den Sie auf der Tastatur machen, im Auge behalten. Alle Daten werden an die Hacker gesendet, die dann verschiedene Algorithmen und Tools einsetzen können, um das Beste aus Ihren Daten herauszuholen. Mit der Zeit erfahren sie verschiedene Dinge über Ihr Verhalten und nicht zuletzt darüber, wo Sie verschiedene Kennwörter verwenden, die Sie auf der Tastatur eingegeben haben. Damit kann dann innerhalb weniger Minuten Ihre gesamte digitale Identität übernommen werden.

Adware ist eine Unterkategorie von Spyware und ist ein Programm, das für Produkte oder Dienstleistungen wirbt. Oft erscheint diese Werbung auch dann noch, wenn das Programm deinstalliert wurde.
Exploitation-Kits sind automatisierte Software, die weniger erfahrene Angreifer bei der Kompromittierung von Systemen unterstützt, indem sie clientseitige Schwachstellen ausnutzt, insbesondere solche in Webbrowsern oder Anwendungen, auf die von Websites aus zugegriffen werden kann; sie stützt sich auf Drive-by-Download-Angriffe, bei denen bösartiger Code in kompromittierte Websites injiziert wird; sie kann Schwachstellen im Browser oder seinen Plugins ausnutzen.

Botnet ist eine Gruppe von Computern, die unter der Kontrolle eines Angreifers stehen; ein Botnet kann für verschiedene Zwecke genutzt werden: Distributed Denial of Service - DDoS-Angriffe, Spamming, Identitätsdiebstahl, Verbreitung von Malware, Infizierung von Computersystemen; sie können auf mehreren Betriebssystemen laufen; 2012 gelang es dem "Flashback"-Botnet, etwa 600.000 Apple-Computer zu infizieren.

Denial of Service ist ein Versuch, die Verfügbarkeit von Computersystemen/-diensten oder elektronischer Kommunikation zu beeinträchtigen. Das Zielsystem wird angegriffen, indem eine sehr große Zahl unzulässiger Anfragen gesendet wird, die seine Hardware- oder Softwareressourcen verbrauchen, so dass es für legitime Nutzer nicht mehr verfügbar ist. Die

Hauptmotivationen für DDoS-Angriffe sind Hacktivismus, Vandalismus und Betrug. Kompromittierung vertraulicher Informationen; bezieht sich auf Datensicherheitsverletzungen, die durch die (absichtliche oder unabsichtliche) Offenlegung vertraulicher Informationen durch interne oder externe Akteure entstanden sind; das Durchsickern von Informationen wird in der Regel durch Hacking, die Verbreitung von Malware, Social-Engineering-Angriffe, physische Angriffe oder den Missbrauch von Privilegien erreicht

Ein besonderer Fall von Rogue Ware/Scareware ist gefälschte Sicherheitssoftware, die, sobald sie im System installiert ist, falsche Sicherheitswarnungen ausgibt und den Benutzer auffordert, ein spezielles Desinfektionsprogramm zu kaufen. Diese Art von Bedrohung verbreitet sich durch verschiedene Methoden wie Social-Engineering-Techniken, Trojaner, Ausnutzung von Schwachstellen (insbesondere Java).

Ransomware ist eine der gefährlichsten und aggressivsten Formen der Internetkriminalität. Die Hacker verwenden einen extrem komplexen Code, um die Funktionalität eines Computers oder eines computergesteuerten Systems zu sperren. Der Besitzer des Systems wird dann von dem Hacker kontaktiert und aufgefordert, ein Lösegeld zu zahlen, um das System wieder zu aktivieren oder Informationen im System "freizuschalten". In den leichten Fällen geht es um Familienfotos oder Firmenkonten, in den schweren Fällen kann es um lebenswichtige Systeme gehen, wie z. B. Kontrollsysteme in Fabriken oder einen mit dem Internet verbundenen Herzschrittmacher.

Arten von Angriffen

Gezielte Angriffe

-eine bestimmte Person oder Organisation ansprechen

-versucht , entweder persönliche/vertrauliche Daten zu sammeln oder die Computersysteme der Zielpersonen zu kompromittieren

hat in der Regel eine Phase, in der sich der Angreifer durch verschiedene Techniken (z.B. Social Engineering) über das anvisierte IT-System informiert und dann den Angriff auslöst

-oft erscheinen seine Handlungen legitim, weil sie von einer vertrauenswürdigen Person zu kommen scheinen

Diebstahl/Verluste/physische Zerstörung

-Aufgrund der zunehmenden Mobilität, die Laptops, Smartphones und Tablets bieten, wird diese Art von Bedrohung bald eine große Rolle spielen.

-konsistente Datensicherung und Inhaltsverschlüsselung können eine Lösung sein, um den tatsächlichen Datenverlust oder die Offenlegung vertraulicher Daten gegenüber Außenstehenden zu begrenzen

Identitätsdiebstahl

-ist eine echte Bedrohung in einem zunehmend online geprägten Umfeld
-Zugangsdaten oder persönliche Daten sind heute das Ziel von Angreifern
-Sobald sie in ihrem Besitz sind, kann der Angreifer betrügerische Transaktionen (insbesondere finanzieller Art) durchführen oder vertrauliche Daten erlangen.

Informationsleck
-beabsichtigte oder unbeabsichtigte Weitergabe von Informationen an eine unbefugte Person
-Informationen wie Geolokalisierung und Telefonbuchkontakte können leicht in die Hände von Angreifern fallen und für betrügerische Zwecke verwendet werden.

Suchmaschinenmanipulation (SEP)
-manipuliert Suchmaschinen, um Suchergebnisse anzuzeigen, die Verweise auf bösartige Websites enthalten. So leitet eine infizierte Webseite die Nutzer auf bösartige Seiten um, und wenn die Opfer die entsprechenden Seiten aufrufen, infizieren sie ihre Computer mit Malware
-Gefälschte digitale Zertifikate
-werden von Angreifern verwendet, um Ressourcen (Websites, Anwendungen, Quellcodes usw.), die in verschiedenen Cyberangriffen verwendet werden, digital zu signieren, damit sie für den Endnutzer unbemerkt bleiben
-werden häufig zum Signieren bösartiger Webanwendungen wie E-Banking oder E-Commerce verwendet, die das HTTPS-Protokoll nutzen
können durch Ausnutzung von Schwachstellen in den PKI-Systemen (Public Key Infrastructure) von Zertifizierungsstellen, die digitale Zertifikate für sichere Websites ausstellen, erstellt oder gestohlen werden.

Sicherer Webserver - SSL

Das Protokoll, das die Verschlüsselung mit öffentlichen Schlüsseln implementiert, heißt SSL (Secure Socket Layer) und wurde von Netscape entwickelt. Dieses Protokoll wird von Browsern und Webservern zur sicheren Datenübertragung verwendet und wurde daher für das HTTP-Protokoll entwickelt.

Die Verbindung zu einem sicheren Webserver wird durch die Angabe des https-Protokolls anstelle von http in der URL hergestellt, d. h. der Zugriff auf die sichere Webseite wird durch das Protokoll und nicht durch den Namen des Servers angezeigt.

Ein sicherer Webserver bietet: Sichere Übertragung von Informationen: Die zwischen dem Server und dem Nutzer übertragenen Daten können nicht entschlüsselt werden, wenn sie abgefangen werden.

Server-Authentifizierung: Wenn der Webserver ein Zertifikat von einer Zertifizierungsstelle (CA) erhalten hat.

Sicherheitscheckliste

Desktop- und mobile Firewall
Beginnen Sie mit der Sicherung Ihrer Außengrenzen, indem Sie sicherstellen, dass Ihre point (digitale Geräte) Firewalls funktionieren. Das hört sich einfach an, aber es sind auch die Grundlagen, mit denen Sie beginnen müssen. In der Regel gibt es drei bis vier verschiedene Arten von Firewalls in Ihrem Netzwerk:
- Firewall auf Ihrem Betriebssystem (Android, iOS, Windows, etc.).
- Firewall in Ihrem Antivirus-/Sicherheitsprogramm.
- Firewall auf Ihrem Internet-Router.
- Firewall auf Ihrer ASA-Box oder einem intelligenten Switch (in der Regel nur größere Unternehmen).

Sicherung
Die Datensicherung sollte eigentlich ganz oben auf der Liste stehen, wie es keine Neuigkeit sein sollte. Ein Backup kann Sie davor bewahren, Lösegeld zahlen zu müssen, um Ihre Daten freizugeben. Die meisten Angriffe mit dieser Art von Malware zielen auf kleine Unternehmen und Privatpersonen ab.

Regeln für sicheres Surfen
-Verwendung der neuesten Browser-Version
-orientieren Sie sich an anderen Browsern (z. B. Google Chrome, Opera, Firefox, Safari usw.), insbesondere beim Zugriff auf potenziell unsichere Webseiten;
-Die meisten Schadprogramme betreffen den Microsoft Internet Explorer (der von über 50 % der Nutzer verwendet wird)
-Prüfen Sie das tatsächliche Ziel der Links, indem Sie den Mauszeiger darüber bewegen und die tatsächliche Adresse im unteren linken Teil des Browsers anzeigen
-Seien Sie vorsichtig, welche Plugins Sie installieren, denn oft sind sie mit bösartiger Software versehen.
klicken Sie nicht auf Links in Pop-up-Fenstern
-Prüfen Sie auf "https://" am Anfang der Webadresse, bevor Sie persönliche Daten eingeben
Beim Online-Einkauf muss der Sicherheitsstufe der Seite größere Aufmerksamkeit gewidmet werden, wenn man sich für die Online-Zahlung mit einer Bankkarte entscheidet.

Senden und Empfangen von E-Mails
-Vermeiden Sie den Versand oder Empfang sensibler Informationen per E-Mail;

-Vermeidung von Social Engineering oder Phishing-Versuchen
Suchen Sie einen E-Mail-Anbieter, der eine starke Anti-Spam-Filterung bietet.
-reagieren Sie nicht auf Spam und vermeiden Sie Kaskaden- oder Pyramiden-E-Mails
-reagieren Sie nicht auf Spam und vermeiden Sie Kaskaden- oder Pyramiden-E-Mails
Verwenden Sie nicht denselben Namen für Ihr privates und Ihr berufliches E-Mail-Konto; die Verwendung unterschiedlicher Namen für diese Konten verringert das Risiko, dass sie Ziel eines Computerangriffs werden
-Vermeiden Sie es, wichtige Informationen in persönlichen E-Mail-Konten oder in anderen Netzwerken außerhalb der Institution/des Unternehmens, in der/dem Sie arbeiten, zu speichern

Die Wahrheit ist, dass die E-Mail noch nie ein sicheres Kommunikationsmedium war. Schließlich müssen sich nur Kriminelle wirklich Gedanken über die Sicherheit ihrer Kommunikation machen. Dies ist eine weit verbreitete, aber völlig falsche Denkweise, und Snowden selbst hat diese Art von Mentalität bekanntlich in Misskredit gebracht.

Die Behauptung, dass einem die Privatsphäre egal ist, weil man nichts zu verbergen hat, ist wie die Behauptung, dass einem die Redefreiheit egal ist, weil man nichts zu sagen hat.

Während viele Menschen immer noch der Meinung sind, dass sie nichts zu befürchten haben, wenn sie nichts zu verbergen haben, gibt es in Wirklichkeit eine Menge Grund zur Besorgnis, und es gibt eine Menge konkreter Gründe, warum Menschen ihre E-Mail-Kommunikation verschlüsseln und ihre Privatsphäre schützen sollten. Das gilt sowohl für Enthüllungsjournalisten, Dissidenten, Whistleblower als auch für normale Durchschnittsbürger.

Warum sollte jemand eine sichere E-Mail versenden?

Schutz vor Bedrohungen durch Cyberkriminelle
Haben Sie schon einmal sensible persönliche Daten in einer E-Mail verschickt und gedacht: "Hoffentlich gerät diese E-Mail nicht in die falschen Hände? Das ist ein wirklich beunruhigender Gedanke, denn wenn jemand anderes als der/die beabsichtigte(n) Empfänger die E-Mail in die Hände bekommt - vor allem, wenn es sich dabei um einen Cyberkriminellen handelt -, könnte das katastrophale Folgen haben.

Das Versenden einer E-Mail mit sensiblen persönlichen Daten wie medizinischen Informationen, Finanzkontodaten, Sozialversicherungsnummern, Adressen oder Telefonnummern kann äußerst riskant sein, da Cyberkriminelle nur eine minimale Menge an persönlichen Daten benötigen, um maximalen Schaden anzurichten. Mit dem Zugriff auf solche sensiblen persönlichen Daten können Cyberkriminelle Ihre Online-Profile kompromittieren, Ihre Bankkonten leerräumen und sogar Ihre Identität stehlen.

Um zu verhindern, dass E-Mail-Anbieter E-Mails überwachen und Daten mit Werbetreibenden teilen

E-Mail-Anbieter sind dafür bekannt, dass sie die E-Mails ihrer Nutzer überwachen und scannen, um gezielte Werbung zu ermöglichen. Obwohl Google Mail im Jahr 2017 anscheinend das Scannen von E-Mails zu Werbezwecken eingestellt hat, bedeutet das nicht unbedingt, dass Google das Scannen von E-Mails zu anderen Zwecken eingestellt hat. Die Funktion "Intelligente Antwort" von Google Mail bietet beispielsweise relevante Vorschläge für schnelle, vorgefertigte Antworten auf eine E-Mail, die Sie erhalten haben, basierend auf dem Inhalt der Nachricht. Wenn Sie also nicht möchten, dass Ihr E-Mail-Anbieter Ihre E-Mail-Nachrichten zu Werbe- oder anderen Zwecken scannt oder überwacht, sollten Sie sichere E-Mails versenden, die den Inhalt dieser Nachrichten effektiv privat halten und für niemanden außer Ihnen und demjenigen, mit dem Sie per E-Mail kommunizieren, zugänglich sind.

Die Massenüberwachung stellt einen Eingriff in unsere bürgerlichen Freiheiten und Grundrechte auf Privatsphäre dar.

Eine solche ungerechtfertigte Überwachung ist ein unangemessener Eingriff in die Privatsphäre und ein direkter Angriff auf unsere bürgerlichen Freiheiten und unser Grundrecht auf Privatsphäre. Wenn Sie eine sichere E-Mail senden, können Sie Ihre Kommunikation verschlüsseln, so dass nur Sie und die andere Partei, mit der Sie sicher kommunizieren, Zugriff auf den Inhalt der Nachricht haben.

Das Versenden einer verschlüsselten E-Mail schützt Ihre Privatsphäre und macht es staatlichen Stellen unmöglich, Ihre sichere E-Mail-Kommunikation zu belauschen. Dies ist vor allem für diejenigen wichtig, deren berufliche Aufgaben absolute Vertraulichkeit in ihrer Kommunikation erfordern, aber auch für alle, die nicht wollen, dass die Regierung ihre Datenschutzrechte mit Füßen tritt.

Zum Schutz vor staatlichen Überwachungsmaßnahmen

Wie wir bereits erwähnt haben, ist die staatliche Massenüberwachung weit verbreitet. Und das gilt nicht nur unter autoritären Regimen wie in China oder im Iran, sondern auch in den Vereinigten Staaten, dem Vereinigten Königreich, Australien, Kanada, Deutschland und anderen westlichen Ländern.

Die Massenüberwachung ist keine Abweichung, sondern die Norm, und sie kann so schädlich sein, dass sie sogar illegal ist.

Aus diesem Grund ist der Versand sicherer E-Mails von entscheidender Bedeutung, vor allem, wenn die von Ihnen gesendete E-Mail sensible persönliche Daten enthält.

Wie man eine sichere E-Mail versendet

Jetzt, da Sie wissen, warum Sie eine sichere E-Mail versenden möchten, wollen Sie vermutlich auch wissen, wie Sie dies tun können. Es gibt verschiedene Möglichkeiten, jede mit bestimmten Vor- und Nachteilen, aber unterm Strich müssen Sie Ihre E-Mail verschlüsseln, wenn Sie eine sichere E-Mail versenden wollen. Wenn Sie eine E-Mail-Nachricht verschlüsseln, verschlüsseln Sie im Wesentlichen den Inhalt dieser Nachricht und machen es für jeden, der den Verschlüsselungsschlüssel nicht hat, unmöglich, die Nachricht zu entschlüsseln.

Welche Möglichkeiten stehen Ihnen zur Verfügung, wenn Sie eine sichere E-Mail versenden möchten?

Verschlüsseln von E-Mails in gängigen E-Mail-Clients

Viele der großen webbasierten E-Mail-Anbieter bieten ihren Nutzern die Möglichkeit, ihre E-Mails mit einem der beiden wichtigsten E-Mail-Verschlüsselungsprotokolle, S/MIME oder OpenPGP, zu verschlüsseln. Der Nachteil ist, dass es nicht immer einfach ist, dies direkt über die Benutzeroberfläche Ihres webbasierten E-Mail-Anbieters zu tun, und dass Sie möglicherweise dafür bezahlen müssen.

Wenn Sie beispielsweise eine sichere E-Mail über Google Mail senden möchten, müssen Sie zunächst die S/MIME-Verschlüsselung aktivieren, indem Sie sich mit einem GSuite-Administratorkonto bei Google Mail anmelden. GSuite-Konten sind in erster Linie für geschäftliche Zwecke gedacht, aber Sie könnten theoretisch auch ein Konto für Ihren persönlichen Gebrauch einrichten. Das andere Problem dabei ist, dass der/die Empfänger, an die Sie E-Mails senden, ebenfalls die S/MIME-Verschlüsselung aktiviert haben müssen, damit dies funktioniert.

Outlook unterstützt ebenfalls die S/MIME-Verschlüsselung, die Sie manuell aktivieren müssen. Zuvor müssen Sie jedoch ein Zertifikat (oder eine digitale ID) vom Administrator Ihres Unternehmens erhalten. Dies ist zugegebenermaßen nicht der einfachste Prozess und für die meisten privaten E-Mail-Benutzer wahrscheinlich auch keine sehr praktische Lösung. Weitere Informationen hierzu finden Sie in unserer Anleitung zur Verschlüsselung von Outlook-E-Mails.

Sie können diese Probleme jedoch umgehen, indem Sie ein kostenloses Drittanbieter-Tool wie Mailvelope installieren, um Ihre E-Mails problemlos zu verschlüsseln. Mailvelope funktioniert mit vielen der beliebtesten E-Mail-Dienste wie Gmail, Yahoo!, Outlook, Hotmail und GMX. Aber auch hier gilt, dass die Empfänger Ihrer verschlüsselten E-Mail-Nachricht eine ähnliche PGP/OpenPGP-Software verwenden müssen, um die E-Mail zu entschlüsseln und den Inhalt zu lesen.

Verwenden Sie einen speziellen sicheren E-Mail-Anbieter

Wenn Sie sich nicht die Mühe machen wollen, die S/MIME- oder OpenPGP-Verschlüsselung in Ihrem herkömmlichen webbasierten E-Mail-Konto manuell zu aktivieren, können Sie viel einfacher eine sichere E-Mail versenden, indem Sie ein Konto bei einem sicheren E-Mail-Anbieter einrichten.

Mit einem sicheren E-Mail-Anbieter wie ProtonMail können Sie sichere, verschlüsselte E-Mails an andere senden, unabhängig davon, ob diese denselben sicheren E-Mail-Anbieter wie Sie verwenden, und Ihr(e) Empfänger können ebenfalls sicher antworten. Viele sichere E-Mail-Anbieter setzen OpenPGP-Verschlüsselung ein, um die E-Mails der Nutzer zu schützen, und ermöglichen es den Nutzern, auf einfache Weise sichere, verschlüsselte E-Mails an andere zu senden und zu empfangen, die in ihren E-Mail-Clients OpenPGP-Verschlüsselung aktiviert haben. Wenn Ihr Empfänger PGP nicht aktiviert hat, können Sie ihm trotzdem eine sichere E-Mail schicken, die nur mit einem gemeinsamen Geheimnis geöffnet werden kann.

Wenn Sie einen sicheren E-Mail-Anbieter nutzen, können Sie sensible Nachrichten ganz einfach durch Verschlüsselung schützen, und das auf einer Plattform, die in der Regel genauso einfach zu bedienen ist wie die großen E-Mail-Anbieter wie Gmail, Yahoo! oder Outlook. Aber im Gegensatz zu diesen großen Anbietern belästigt ein sicherer E-Mail-Anbieter Sie nicht mit Werbung oder überwacht Ihre E-Mails (da er dank der Ende-zu-Ende-Verschlüsselung nicht einmal auf sie zugreifen kann).

Der Nachteil ist, dass Sie für den vollen Funktionsumfang eines sicheren E-Mail-Anbieters, den erweiterten Speicherplatz und die uneingeschränkte Nachrichtenübermittlung bezahlen müssen. Viele der besten sicheren E-Mail-Anbieter bieten jedoch eine kostenlose Stufe (mit bestimmten Einschränkungen) an, mit der Sie kostenlos sichere E-Mails senden und empfangen können. Wenn Sie nur eine begrenzte Anzahl sicherer E-Mails versenden möchten, ist die kostenlose Option sicherlich eine praktikable Lösung, aber wenn Sie planen, den Großteil Ihrer E-Mail-Korrespondenz auf sichere Weise abzuwickeln, müssen Sie ein Premium-Abonnement erwerben.

Wenn Sie eine E-Mail erhalten, achten Sie auf Folgendes

-Identität des Absenders ist nicht garantiert: Es wird die Beziehung zwischen dem Absender und dem Inhalt der Nachricht überprüft;

-Öffnen Sie keine Anhänge, die von unbekannten Personen stammen oder mit legitimen Konten verbunden sind, aber Nachrichten mit verdächtigem Betreff und Inhalt enthalten. Sie können bösartige Software (Malicious Software oder Malware, wie Würmer, Trojaner, Spyware, Formen von Adware usw.) enthalten;

-Wenn es unbedingt notwendig ist, einen Anhang zu öffnen, auch von legitimen E-Mails, muss er zuerst heruntergeladen und mit der installierten Antivirenlösung gescannt und dann mit der zugehörigen Anwendung geöffnet werden;

-Links in E-Mails sollten nicht direkt im Text der Nachricht aufgerufen werden; möglicherweise kann der Link kopiert und in einem anderen Browser-Tab geöffnet werden;

Antworten Sie nicht auf E-Mails, in denen Sie um persönliche oder vertrauliche Daten gebeten werden (z. B. PIN-Code und Bankkartennummer).

Woher wissen Sie, dass Ihre E-Mail von Unbekannten "abgerufen" wurde?

-Ihre Kontakte melden, dass sie Spam-E-Mails von Ihnen erhalten haben;

-Sie erhalten viele E-Mails mit Fehlern;

-Nachrichten erscheinen im Ordner "Gesendet", ohne dass Sie sie gesendet haben;

-Der Verlauf des Kontostandorts bei der Anmeldung stimmt nicht mit Ihrer aktuellen Aktivität überein.

Passwortsicherheit. Die Angriffe zielen darauf ab, das Passwort zu identifizieren und auf die durch dieses Passwort eingeschränkten Informationen zuzugreifen. Die am häufigsten verwendeten Angriffsmethoden dieser Art sind "Wörterbuchangriffe" und "Brute Force".

Ein "Wörterbuchangriff" zielt auf den unbefugten Zugriff auf bestimmte Ressourcen oder Computersysteme ab, indem nacheinander die Passwörter/Entschlüsselungsschlüssel ausprobiert werden, die in einer vordefinierten Liste von Wörtern oder Sätzen enthalten sind.

Ein "Brute-Force"-Angriff ist eine Methode des unbefugten Zugriffs auf ein Computersystem oder der Entschlüsselung verschlüsselter Inhalte (z. B. Passwörter) durch "Brute-Force"-Berechnung - durch Programme, die die Trial-Error-Methode anwenden. Die Methode besteht darin, nacheinander alle möglichen Zeichenkombinationen auszuprobieren, ohne einen ausgeklügelten Algorithmus zu verwenden.

Maßnahmen: Captcha-System, Zugriffszeit nach einer Reihe von fehlgeschlagenen Zugriffen.

-Verwenden Sie eindeutige IDs und Passwörter und geben Sie diese nicht an andere Benutzer weiter;

-Länge und Komplexität des Passworts müssen so gewählt werden, dass es schwer zu erraten, aber leicht zu merken ist;

-Regelmäßige Änderung der Passwörter (in Abständen von 1-3 Monaten);

-Verwendung verschiedener Passwörter für verschiedene Anwendungen;

-die Verwendung mehrerer Authentifizierungsmethoden (PIN, Fingerabdruck, Warnmeldungen usw.);

-Vermeidung der Verwendung ähnlicher Passwörter zu Hause und am Arbeitsplatz.

Nicht verwenden:

-den Namen von dir, einem anderen Familienmitglied oder deinem Lieblingstier,

-Elemente Ihrer Adresse: Gebäudename, Straße, Land,

-den Namen der Einrichtung, des Projekts usw.,

-Rufnummer, Registrierungsnummer

-den Namen des Lieblingsstars oder der Lieblingsfigur (oder des Films, Buchs usw.),

-Wörterbuch ;

-den Namen des Kontos, für das Sie das Kennwort festlegen;

Methoden, die ein falsches Gefühl von sicheren Passwörtern vermitteln

-phonetische Methode: "Ich weiß sicher, dass ich eine Blu-Ray DVD habe!": St1u100%km1DVDBLr!

-Methode des ersten Buchstabens: "Ich weiß sicher, dass ich eine Blu-Ray DVD habe!": "sSka1DVDBr!"

-Substitutionsmethode (in der Regel Vokale): Ersetzen Sie bestimmte Buchstaben durch Zahlensymbole innerhalb eines Wortes. Ändern Sie zum Beispiel Apfel in @ppl3.

-Umkehr- und Substitutionsmethode: "Ich liebe Urlaube": "r0d@3l11d3cn0c"

-Groß-/Kleinschreibung, Zahl/Symbol und Ersetzungsmethode: "Ich liebe Urlaub": "@D0rC)nC3d11L3"

-Anpassung der Methoden je nach Website, um ein persönliches Passwort-Generierungssystem zu erstellen: Gmail - "G@D0rC)nC3d!1L3MAIL", Yahoo - "YA@D0rC)nC3d!1L3HOO", Wizzair - "WIZZ@D0rC)nC3d!1L3AIR".

Verwenden Sie diese Methoden nicht! Während sie früher die Norm waren, wurden sie aufgrund der CPU-Leistung weitgehend irrelevant. Die heutigen Tools zum Knacken von Passwörtern verringern die Wirksamkeit der oben genannten Methoden.

Eine bessere Methode zur Erstellung von Passwörtern besteht darin, ganze Sätze zu verwenden und dabei Groß- und Kleinbuchstaben, Zahlen und vorzugsweise Sonderzeichen einzubeziehen. Auf diese Weise brauchen automatisierte Skripte, die einfach archaische Methoden wie die besprochenen verwenden, einen enormen Aufwand, um Ihr Passwort zu erzwingen oder zu erraten. Die neue Methode heißt "Passphrasen" und kann bis zu 100 Zeichen oder mehr umfassen.

Die Passphrase gilt als besser als das Passwort, weil sie leichter zu merken und schwerer zu knacken ist. Es ist einfacher, sich eine zufällige Phrase mit 4 bis 8 Wörtern zu merken als eine komplexe Zeichenfolge aus Buchstaben, Zahlen und Sonderzeichen mit 30 Zeichen. Selbst die fortschrittlichsten Tools zum Knacken von Passwörtern sind nicht in der Lage, eine Passphrase zu knacken, die zufällige Wörter verwendet und eine signifikante Länge hat.

Wie man eine Passphrase erstellt

- Kombinieren Sie eine Wortgruppe zu einem Satz, der für Sie einen Sinn ergibt, aber nicht für andere.
- Verwenden Sie keine allgemeinen Phrasen oder berühmten Zitate
- Leerzeichen innerhalb und zwischen den Wörtern hinzufügen
- Verwenden Sie Großbuchstaben und schreiben Sie einige der Wörter groß.
- Fügen Sie Satzzeichen und Sonderzeichen hinzu, die für Sie sinnvoll sind
- Ungewöhnliche Schreibweisen von Wörtern verwenden

Eine weitere Möglichkeit, eine Passphrase zu entwickeln, ist die Verknüpfung mit einer persönlichen Geschichte oder einer privaten Erinnerung. Schlüsselwörter können verwendet werden, um die Geschichte zu erzählen.

Insgesamt wird in diesem Modul der Einheit

Wie Sie die Cyber Kill Chain effektiv in Ihrer Cybersicherheitsstrategie nutzen können

Erkennen - Analysieren und Auffinden von Einbruchsversuchen.

Verweigern - Stoppen Sie die Angriffe, sobald sie stattfinden.

Unterbrechen - Stoppt die Datenübertragung

Degrade - Die Wirksamkeit des Angriffs verringern und einschränken.

Täuschen - Führt die Angreifer in die falsche Richtung.

Eindämmen - Verbergen und begrenzen Sie die Reichweite des Angriffs, so dass er nur einen Teil des Unternehmens betrifft.

Fragen:

Fragen Diskussionsforum, die mit einer kurzen Erklärung beantwortet werden müssen. Die Antworten werden mit dem Mentor während der Mentoring-Sitzungen besprochen

-Was ist Malware

-Welche sind die wichtigsten Cyber-Bedrohungen

-Welche Rolle spielt ein sicherer Webserver - SSL

-Erklären Sie einige Regeln für sicheres Surfen

-Vorstellung einiger Maßnahmen zum sicheren Senden und Empfangen von E-Mails

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

-Malware

- Die wichtigsten Cyber-Bedrohungen

-Regeln für sicheres Surfen

-Maßnahmen zur Sicherung des Versands und Empfangs von E-Mails

Anhänge (PowerPoint-Präsentation, Handouts, Ausdrucke, Links, Video...):
Siehe Powerpoint- und Videodateien

Referenzen:

-Was ist Cybersicherheit?

URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

-Malware oder bösartige Software

URL: https://www.malwarebytes.com/malware

-Cybersicherheit für alle.

https://www.avast.com/c-malware

-Malware-Entfernungssoftware 2022; Sichern Sie Ihre persönlichen Daten

URL: Malware

-Was sind Bedrohungen der Cybersicherheit?

URL: https://www.imperva.com/learn/application-security/cyber-security-threats/

-21 Top-Bedrohungen für die Cybersicherheit und wie Threat Intelligence helfen kann

URL: https://www.exabeam.com/information-security/cyber-security-threat/

-E-Mails senden und empfangen

URL: https://www.ibm.com/docs/en/i/7.1?topic=mail-sending-receiving-e

-Erstellen und Versenden von E-Mails

URL: https://support.google.com/a/users/answer/9259846?hl=en

Die Cyber Kill Chain: Die sieben Schritte eines Cyberangriffs

URL: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/