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

InCyT træningsmoduler

Informationssikkerhed for ledere Enhed 3 – uge 5 Enhedens (modul) navn: Information Security Management 3	
Læringsaktiviteter	❑ **Webinar** ❑ **Øvelser** ❑ **Værksted** ❑ **Præsentation** ❑**Andet**
Læringsansvarlig	• George Matache et al.
Læringsaktivitetsmål	1 Generel terminologi 2. Fortrolighed, integritet og tilgængelighed (CIA) 3. Regler og standarder 4. Informationssikkerhedsstyring 5. Hvordan virker malware? 6. Top cybertrusler 7. Typer af angreb 8. Sikker webserver – SSL 9. Afsendelse og modtagelse af e-mails 10. Asset management
Færdigheder, der skal opnås	• TS3 netværkssikkerhed • TS4 Penetration (udnyttelige sårbarheder) test • SS3 Kognitiv og adfærdsanalyse
Varighed af læringsaktivitet	2 uger
Læring krav	***Hvad skal der til?***
	• Internetadgang • Internet browser • MS Office365

Kort information om modulet

Beskrivelse
Cybersikkerhed er praksis med at forsvare computere, servere, mobile enheder, elektroniske systemer, netværk og data mod ondsindede angreb. Det er også kendt som informationsteknologisikkerhed eller elektronisk informationssikkerhed. Udtrykket gælder i en række forskellige sammenhænge, fra erhvervslivet til mobil databehandling, og kan opdeles i et par almindelige kategorier. Virksomheder er ofte så optaget af deres daglige drift, at de glemmer at investere kraftigt i netværkssikkerhed. Andre forstår behovet for omfattende netværkssikkerhed, men har en lempelig strategi i forhold til deres it, hvilket kan være lige så skadeligt i tilfælde af et datalæk. At forstå, hvad netværkssikkerhed indebærer, samt den bedste praksis, som du kan overholde, som sikrer, at din virksomheds netværk er sikkert mod de mange udefrakommende trusler, der ønsker at infiltrere dit netværk, er afgørende for at holde dine data, og i sidste ende din virksomhed, sikker. Det er yderst vigtigt, at uddannelsen i cybersikkerhed for SMV'er - ledere og medarbejdere - er konkret og interaktiv - også har hands-on, fordi de små SMV'er ikke har tid, motivation eller ressourcer til at bruge på dette emne, hvorfor det er meget vigtigt at uddannelsen er relevant og overskuelig for de ledere, der deltager. Derfor planlægges dette modul på baggrund af dette. Informationssikkerhedsstyring (ISM) definerer og administrerer kontroller, som en organisation skal implementere for at sikre, at den på fornuftig vis beskytter aktivers fortrolighed, tilgængelighed og integritet mod trusler og sårbarheder. Malware eller "ondsindet software" er et paraplybegreb, der beskriver ethvert ondsindet program eller kode, der er skadelig for systemer. Fjendtlig, påtrængende og bevidst ubehagelig malware søger at invadere, beskadige eller deaktivere computere, computersystemer, netværk, tablets og mobile enheder, ofte ved at tage delvis kontrol over en enheds drift. Ligesom den menneskelige influenza forstyrrer den normal funktion. Motiverne bag malware varierer. Malware kan handle om at tjene penge på dig, sabotere din evne til at få arbejdet udført, at lave en politisk udtalelse eller bare prale. Selvom malware ikke kan beskadige den fysiske hardware i systemer eller netværksudstyr, kan den stjæle, kryptere eller slette dine data, ændre eller kapere kernecomputerfunktioner og spionere på din computeraktivitet uden din viden eller tilladelse. Malware er beskrevet og defineret, introducerer dens mange forskellige typer og forklarer, hvordan det virker. Vi beskriver også advarselstegnene på en inficeret enhed og forklarer, hvordan man forhindrer det. Eleverne kunne blive informeret om sådanne aspekter ved at læse den tilsvarende tekst, se streaming-webinarer og løse øvelser i eget tempo og gennem live publikumsinteraktion med kontinuerlig feedback og kontrol af gamification-viden.

Lærematerialets indhold

Især hvis du har en virksomhed, der er meget afhængig af, at dine it-systemer fungerer og er sikre. Cybersikkerhedstrusler er stigende.

Cyberangreb fortsatte med at stige i EU i 2020 og 2021 og især 2022, både med hensyn til deres sofistikerede og antal, og med hensyn til deres virkning. EU arbejder på flere fronter for at beskytte borgere og virksomheder mod cyberkriminalitet og for at sikre et sikkert, åbent og sikkert cyberspace.

I 2022 vil vi se statssponsorerede grupper rettet mod kryptovalutaindustrien, mens cyberkriminelle vil drage fordel af investorer ved at lave digitale tegnebøger med indbyggede bagdøre. Vi vil sandsynligvis se en stigning i angreb mod betalingssystemer og mere avancerede mobile trusler.

Cirka halvdelen (47 pct.) af befolkningen (i Danmark) mellem 16 og 89 år har haft cyberkriminalitet tæt inde på livet i form af falske e-mails, bedrageri, hacking eller identitetstyveri. Det samme gælder 11 pct. af danske private virksomheder. 8 pct. af virksomhederne har oplevet, at adgangen til digitale tjenester er blevet spærret og 3 pct. har fået slettet eller ødelagt data. Phishing er det mest udbredte problem, men desværre ser vi også en radikal stigning i antallet af falske hjemmesider i takt med, at flere og flere handler og arbejder hjemmefra.

Kernen i ISM omfatter informationsrisikostyring, en proces, der involverer vurdering af de risici, en organisation skal håndtere i forvaltningen og beskyttelsen af aktiver, samt formidling af risici til alle relevante interessenter. Dette kræver korrekt aktividentifikation og værdiansættelsestrin, herunder evaluering af værdien af fortrolighed, integritet, tilgængelighed og udskiftning af aktiver. Som en del af informationssikkerhedsstyring kan en organisation implementere et informationssikkerhedsstyringssystem og andre bedste praksisser, der findes i ISO/IEC 27001, ISO/IEC 27002 og ISO/IEC 27035-standarderne om informationssikkerhed. Men denne form for certificering er ofte for ressourcekrævende for SMV'er, hvorfor vi forbereder os på en agil cybersikkerhedspraksis:

Informationssikkerhed og interne kontrolsystemer

- Generel terminologi
- CIA-triade
- Anatomi af et angreb (angrebsoverfladereduktion)
- Cybersikkerhedsrammer

Informationssikkerhedsstyring
E-mail og kontor
Enheder

En vigtig udfordring for SMV'erne er malware, som er en paraplybetegnelse for enhver form for "ondsindet software", der er designet til at infiltrere din enhed uden din viden. Der er mange typer malware, og hver af dem fungerer forskelligt i forfølgelsen af sine mål. Men alle malware-varianter deler to definerende træk: de er luskede, og de arbejder aktivt imod dine interesser.

Er malware en virus? Ja og nej. Mens alle computervirus er malware, er ikke alle malware virus. Virus er kun én type malware. Du vil høre mange mennesker bruge de to udtryk i flæng, men fra et teknisk synspunkt er vira og malware ikke det samme.
Tænk over det på denne måde: Malware er ondsindet kode. Computervirus er ondsindet kode, der spredes på tværs af computere og netværk.

Hvordan virker malware?

Al malware følger det samme grundlæggende mønster: Brugeren downloader eller installerer uforvarende malwaren, som inficerer enheden.

De fleste malware-infektioner opstår, når du utilsigtet udfører en handling, der får malwaren til at blive downloadet. Denne handling kan være at klikke på et link i en e-mail eller besøge et ondsindet websted. I andre tilfælde sprederhackere malware gennem peer-to-peer fildelingstjenester og gratis softwaredownload-pakker. Indlejring af en smule malware i en populær torrent eller download er en effektiv måde at sprede det over en bred brugerbase. Mobile enheder kan også blive inficeret via tekstbeskeder.

En anden teknik er at indlæse malware i firmwaren på en USB-stick eller et flashdrev. Fordi malwaren er indlæst på enhedens interne hardware (i stedet for dens fillager), er det usandsynligt, at din enhed opdager malwaren. Det er derfor, du aldrig bør indsætte et ukendt USB-drev i din computer.

Når malwaren er blevet installeret, inficerer den din enhed og begynder at arbejde mod hackernes mål. Det, der adskiller de forskellige typer malware fra hinanden, er, hvordan de gør dette. Så hvordan virker malware? Hvad er et malware-angreb?

Top cybertrusler

Drive-by exploits kan automatisk udnytte eksisterende sårbarheder i software installeret på en pc uden at interagere med den legitime bruger; de udvidede deres anvendelsesområde i 2012 til også at omfatte mobile terminaler. den fokuserer næsten udelukkende på at kompromittere legitime websteder. sårbarheder i browseren, dens plugins eller operativsystemet kan udnyttes til at

installere malware på pc'en uden brugerens viden, infektionen kan startes ved simpel internet-browsing.
Orme er selvreplikerende programmer; bruge netværket af computere til at sende deres egne kopier til andre noder (computere i netværket), formå at gøre dette uden indblanding fra nogen bruger, i modsætning til en computervirus behøver en computerorm ikke at være knyttet til et eksisterende program, det forårsager skade på netværket, selv bare ved at optage båndbredde.

Trojan præsenterer sig selv i form af legitime programmer, som i virkeligheden er skabt med det formål at stjæle fortrolige data eller give uautoriserede brugere eller programmer adgang til det inficerede system; udgør langt de fleste infektioner (80%).

Malware repræsenterer ethvert program, hvis funktion er at forårsage software- eller hardwareskade på en computer (f.eks. vira) – som beskrevet ovenfor.

Trackware er de programmer, der bruger nogle sårbarheder i webbrowseren til at sende en server eller personer oplysninger om de websteder, man får adgang til, den søgte information og brugerens browservaner; Virus har til formål at inficere så mange personlige computere som muligt, mens spyware sigter mod at sprede sig over internettet, vira har normalt en farlig nyttelast, de ønsker at forårsage skade på den inficerede computer, mens spyware kun bremser computerens processer, tilføjer popups og destabiliserer browser og har andre "irriterende" effekter.

SQL Injection (Code Injection) opstår, når en angriber kan indsætte data i en SQL-forespørgsel sendt til en database; ved at injicere syntaksen, modificeres sætningens logik, så den udfører en anden handling, er den mest almindelige sårbarhed. Den bedste SQL-injection - forsvarsstrategi er baseret på implementering af stærke inputvalideringsrutiner, så angriberen ikke kan indtaste andre data, end applikationen har brug for.

Spyware er generelt defineret som et program, der udnytter sårbarhederne i et system til gavn for en tredjepart, det kan gøre din computer langsommere, gøre den sårbar over for virusinfektion og indsamle fortrolige oplysninger såsom brugernavne til forskellige applikationer, adgangskoder og kreditkort/bankkontooplysninger.

En keylogger er et lille "smart" program, som hackere placerer på din computer, uden at du opdager det. Her kan den ligge i flere måneder eller år og holde øje med hvert eneste tastetryk du laver på tastaturet. Al data sendes til hackerne, som så kan bruge forskellige algoritmer og værktøjer til at få det bedste ud af dine data. Med tiden finder de ud af forskellige ting om din adfærd og ikke mindst hvor du bruger forskellige adgangskoder, du har indtastet på tastaturet. Det kan så bruges til at overtage hele din digitale identitet i løbet af få minutter.

Adware er en underkategori af spyware og er et program, der reklamerer for produkter eller tjenester. Ofte vises disse annoncer, selv efter at programmet er blevet afinstalleret.
Udnyttelsessæt er automatiseret software, der hjælper mindre erfarne angribere med at kompromittere systemer ved at udnytte sårbarheder på klientsiden, især dem i webbrowsere eller applikationer, som websteder kan få adgang til; er afhængig af drive-by download-angreb, hvor ondsindet kode injiceres på kompromitterede websteder; kan udnytte sårbarheder i browseren eller dens plugins.

Botnet repræsenterer et sæt computere, der er under kontrol af en angriber; Et botnet kan bruges til flere formål: Distribueret Denial of Service - DDoS-angreb, spamming, identitetstyveri, malware-distribution, inficering af computersystemer; de kan køre på flere operativsystemer; i 2012 lykkedes det "Flashback"-botnettet at inficere cirka 600.000 Apple-computere.

Denial of Service er et forsøg på at påvirke tilgængeligheden af computersystemer/tjenester eller elektronisk kommunikation. Målsystemet angribes ved at sende et meget stort antal illegitime anmodninger, som opbruger dets hardware- eller softwareressourcer, hvilket gør det utilgængeligt for legitime brugere. De vigtigste motiver for DDoS-angreb er hacktivisme, hærværk og bedrageri. Kompromittering af fortrolige oplysninger; henviser til datasikkerhedsbrud, der er opstået gennem offentliggørelse (uanset om det er forsætligt eller utilsigtet) af fortrolige oplysninger fra interne eller eksterne agenter; Informationslækage opnås normalt gennem hacking, malware-distribution, social engineering-angreb, fysiske angreb eller misbrug af privilegier

Rogue ware/scareware er en type trussel, der tager form af falsk software; Et særligt tilfælde af rogue ware/scareware er falsk sikkerhedssoftware, som en gang installeret i systemet giver falske sikkerhedsadvarsler og inviterer brugeren til at købe et særligt desinfektionsværktøj. Denne type trussel forplanter sig gennem forskellige metoder såsom social engineering-teknikker, trojanske heste, udnyttelse af sårbarheder (især java).

Ransomware er en af de farligste og mest aggressive former for cyberkriminalitet. Hackerne bruger et stykke ekstremt kompleks kode til at låse funktionaliteten af en computer eller et computerstyret system. Ejeren af systemet bliver derefter kontaktet af hackeren med et krav om løsesum for at genaktivere systemet eller "låse op" oplysninger i systemet. I de milde tilfælde drejer det sig om familiebilleder eller virksomhedens regnskaber, i de alvorlige tilfælde kan det dreje sig om vitale systemer som f.eks.; kontrolsystemer på fabrikker, eller en internetforbundet pacemaker.

Typer af angreb
Målrettede angreb
- målrette sig mod en bestemt person eller organisation

- sigter mod enten at indsamle personlige/fortrolige data eller kompromittere målcomputersystemer
- generelt har en fase, hvor angriberen informerer sig selv gennem forskellige teknikker (f.eks. social engineering) om det målrettede it-system og derefter udløser angrebet
- ofte forekommer hans handlinger legitime, fordi de ser ud til at komme fra en troværdig person

Tyveri/Tab/Fysisk ødelæggelse

- på grund af den øgede mobilitet, som bærbare computere, smartphones eller tablets tilbyder, er denne type trussel ved at blive en stor trussel
- konsekvent datasikkerhedskopiering og indholdskryptering kan være en løsning til at begrænse faktiske datatab eller videregivelse af fortrolige data til udefrakommende

Identitetstyveri

- er en reel trussel i et stadig mere online miljø
- adgangsoplysninger eller personlige data er målet for angribere i dag
- når den først er i deres besiddelse, kan angriberen udføre svigagtige transaktioner (især økonomiske) eller indhente fortrolige data

Informationslæk

- forsætlig eller utilsigtet videregivelse af oplysninger til en uautoriseret person
- oplysninger såsom geolokation og telefonbogskontakter kan nemt falde i hænderne på angribere og blive brugt til svigagtige formål

Søgemaskinemanipulation (SEP)

- manipulerer søgemaskiner til at vise søgeresultater, der indeholder referencer til ondsindede websteder. Således omdirigerer en inficeret webside brugerne til ondsindede websteder, og hvis ofrene får adgang til de respektive websteder, inficerer de deres computere med malware
- Falske digitale certifikater
- bruges af angribere til digitalt at signere ressourcer (websteder, applikationer, kildekoder osv.), der bruges i forskellige cyberangreb for at videregive uopdagelige til slutbrugeren
- bruges ofte til at signere ondsindede webapplikationer såsom e-banking eller e-handel, som bruger HTTPS-protokollen
- kan skabes eller stjæles ved at udnytte sårbarheder i PKI-systemerne (Public Key Infrastructure) hos certificeringsmyndigheder, der udsteder digitale certifikater til sikre websteder.

Sikker webserver – SSL

Protokollen, der implementerer offentlig nøglekryptering, kaldes SSL (Secure Socket Layer), udviklet af Netscape. Denne protokol bruges af browsere og webservere til at overføre data sikkert, så den blev oprettet til at blive brugt af HTTP-protokollen.

Tilslutning til en sikker webserver sker ved at nævne https-protokollen i stedet for http i URL'en - det vil sige, at adgang til den sikre webside er angivet af protokollen, og ikke navnet på serveren.

En sikker webserver tilbyder: Sikker overførsel af information: de data, der transmitteres mellem serveren og navigatoren, kan ikke dekrypteres i tilfælde af at de bliver opfanget.
Servergodkendelse: Hvis webserveren har modtaget et certifikat fra en certificeringsmyndighed (CA).

Sikkerhedstjekliste

Desktop og mobil firewall
Start med at sikre dine ydre omkredse ved at sørge for din end
point's (digitale enheders) firewalls virker. Det lyder grundlæggende, men det er også i det helt basale, du skal i gang. Der er typisk tre til fire forskellige typer firewalls på dit netværk:
• Firewall på dit operativsystem (Android, iOS, Windows osv.).
• Firewall på dit antivirus/sikkerhedsprogram.
• Firewall på din internetrouter.
• Firewall på din ASA-boks eller intelligente switch (Typisk kun større virksomheder).

Backup
Backup burde virkelig være øverst på listen, ligesom det ikke burde være nyheder. Sikkerhedskopiering kan spare dig for at skulle betale en løsesum for at få dine data låst op. Tag dog ikke fejl af virksomhedens størrelse, de fleste af angrebene med denne type malware er rettet mod små virksomheder og enkeltpersoner.

Regler for sikrere browsing
- Brug den seneste browserversion
- orienter dig mod andre typer browsere (f.eks . Google Chrome, Opera, Firefox, Safari osv.), især når du får adgang til potentielt usikre websider;
- det meste af malware påvirker Microsoft Internet Explorer (bruges af over 50 % af brugerne)
- kontroller den rigtige destination for links ved at føre musemarkøren hen over den og se den rigtige adresse i den nederste venstre del af browseren
- vær forsigtig med hvilke plugins du installerer, ofte kommer de med skadelig software
- klik ikke på links i pop op-vinduer
- tjek efter "https://" i begyndelsen af webadressen, før du indtaster personlige oplysninger

- i forbindelse med at foretage et onlinekøb, skal der være større opmærksomhed på sidens sikkerhedsniveau, hvis man vælger online betaling med bankkort

Afsendelse og modtagelse af e-mail

- undgå at sende eller modtage følsomme oplysninger via e-mail;
- undgå social engineering eller phishing-forsøg
- se efter en e-mail-udbyder, der tilbyder stærk anti-spam-filtrering
- Reager ikke på spam og undgå kaskade- eller pyramidemails
- Reager ikke på spam og undgå kaskade- eller pyramidemails
- Brug ikke det samme navn til din personlige og arbejds-e-mail-konto; brugen af distinkte navne for disse konti reducerer risikoen for, at de bliver mål for et computerangreb
- undgå at opbevare kritiske oplysninger på personlige e-mail-konti eller i andre netværk uden for den institution/virksomhed, hvor du arbejder

Sandheden er, at e-mail aldrig traditionelt har været et sikkert medie til kommunikation. Det er trods alt kun kriminelle, der virkelig skal bekymre sig om at sikre deres kommunikation. Dette er en ekstremt almindelig, men alligevel fuldstændig mangelfuld måde at tænke på, og Snowden selv har berømt miskrediteret denne type mentalitet.

At argumentere for, at man er ligeglad med privatlivets fred, fordi man ikke har noget at skjule, er som at argumentere for, at man er ligeglad med ytringsfriheden, fordi man ikke har noget at sige.

Mens mange mennesker måske stadig abonnerer på den tankegang, at de ikke har noget at være bekymrede over, hvis de ikke har noget at skjule, er virkeligheden, at der er masser at være bekymret over, og der er masser af konkrete grunde til, at folk skal kryptere deres e-mail-kommunikation og beskytte deres privatliv. Dette gælder uanset om du er en undersøgende journalist, dissident, whistleblower eller bare en almindelig gennemsnitsborger.

Hvorfor skulle nogen sende en sikker e-mail?

For at beskytte mod trusler fra cyberkriminelle
Har du nogensinde sendt følsomme personlige oplysninger i en e-mail og tænkt, 'velp, jeg håber bestemt, at den e-mail ikke på en eller anden måde ender i de forkerte hænder? Dette er en virkelig foruroligende tanke, for hvis en anden end den/de tilsigtede modtager(e) får fingrene i e-mailen – især hvis denne nogen tilfældigvis er en cyberkriminel – kan resultaterne potentielt være katastrofale.

Det kan være ekstremt risikabelt at sende en e-mail, der indeholder følsomme personlige data som dine medicinske oplysninger, finansielle kontooplysninger, personnummer, adresse eller

telefonnummer, fordi cyberkriminelle kun behøver en minimal mængde personlige data for at kræve maksimal skade. Med adgang til følsomme personlige data som denne kan cyberkriminelle kompromittere dine onlineprofiler, dræne dine bankkonti og endda stjæle din identitet.

For at forhindre e-mail-udbydere i at overvåge e-mails og dele data med annoncører
E-mail-udbydere har været kendt for at overvåge og scanne brugernes e-mail-beskeder for at lette målrettede annonceringsindsatser. Selvom Gmail i 2017 tilsyneladende holdt op med at scanne e-mails til reklameformål, betyder det ikke nødvendigvis, at Google er holdt op med at scanne e-mails til andre formål. For eksempel tilbyder Gmails "Smart Reply"-funktion relevante forslag til hurtige, standardsvar på en e-mail, du har modtaget, baseret på indholdet af dens meddelelse. Så hvis du ikke ønsker, at din e-mail-udbyder skal scanne eller overvåge dine e-mails til annoncering eller andre formål, så vil du gerne sende sikre e-mails, der effektivt holder indholdet af disse beskeder privat og utilgængeligt for andre end dig og den part, du kommunikerer med via e-mail.

Masseovervågning griber ind i vores borgerlige frihedsrettigheder og grundlæggende rettigheder til privatlivets fred.
En sådan uberettiget overvågning er unødigt invasiv og en direkte krænkelse af vores borgerlige frihedsrettigheder og vores grundlæggende rettigheder til privatlivets fred. Når du sender en sikker e-mail, kan du kryptere din kommunikation, så kun du og den anden part, du kommunikerer sikkert med, kan få adgang til indholdet af beskeden.

At sende en krypteret e-mail bevarer dit privatliv og gør det effektivt umuligt for offentlige enheder at snuse efter din sikre e-mail-kommunikation. Dette er især vigtigt for dem, hvis jobansvar kræver fuldstændig fortrolighed i deres kommunikation, men det er også vigtigt for alle, der generelt ikke ønsker, at regeringen træder på deres privatlivsrettigheder.

For at beskytte mod regeringens overvågningsindsats
Som vi nævnte tidligere, er massemyndighedens overvågningspraksis omfattende. Og det gælder ikke kun under autoritære regimer som i Kina eller Iran, men også i USA, Storbritannien, Australien, Canada, Tyskland og andre vestlige lande.
Masseovervågning er ikke en aberration, det er normen, og det kan være skadeligt, så det er ulovligt.

Derfor er det vigtigt at sende sikre e-mails, især hvis den e-mail, du sender, indeholder følsomme personlige oplysninger.

Sådan sender du en sikker e-mail

Nu hvor du kender grundene til, at du gerne vil sende en sikker e-mail, gætter vi på, at du sikkert vil vide, hvordan du rent faktisk gør det. Der er et par måder at gøre det på, hver med visse iboende fordele og ulemper, men bundlinjen er, at hvis du vil sende en sikker e-mail, så skal din e-mail-besked krypteres. Når du krypterer en e-mail-meddelelse, krypterer du i det væsentlige indholdet af den meddelelse og gør det umuligt for nogen uden krypteringsnøglen at afkode meddelelsen.

Hvilke muligheder er tilgængelige for dig, hvis du vil sende en sikker e-mail?

Krypter e-mails i populære e-mail-klienter
Mange af de store web-baserede e-mail-udbydere vil tillade brugere at kryptere deres e-mails ved hjælp af enten en af de to primære e-mail-krypteringsprotokoller, S/MIME eller OpenPGP. Ulempen er, at det måske ikke altid er en enkel eller ligetil proces at gøre det direkte fra din webbaserede e-mail-udbyders grænseflade, og du skal muligvis betale for det.

Hvis du f.eks. vil sende en sikker e-mail på Gmail, skal du først aktivere S/MIME-kryptering ved at logge på Gmail med en GSuite-administratorkonto. GSuite-konti er primært til forretningsformål, men du kan teoretisk set oprette en konto til dit personlige brug. Det andet problem med dette er, at den eller de modtagere, du e-mailer, også skal have S/MIME-kryptering aktiveret, for at dette kan fungere.

På samme måde understøtter Outlook også S/MIME-kryptering, og du skal aktivere den manuelt, men før du gør det, skal du anskaffe et certifikat (eller digitalt ID) fra din organisations administrator. Dette er ganske vist ikke den mest strømlinede proces, og det vil sandsynligvis heller ikke være en meget praktisk løsning for de fleste personlige e-mail-brugere. Se vores, hvordan du krypterer Outlook-e-mails for at få flere oplysninger om dette.

Du kan dog omgå disse problemer ved at installere et gratis tredjepartsværktøj som Mailvelope for at kryptere dine e-mails med lethed. Mailvelope fungerer med mange af de mest populære e-mail-tjenester som Gmail, Yahoo!, Outlook, Hotmail og GMX. Men igen, modtageren(e) af din krypterede e-mail-meddelelse skal også bruge lignende PGP/OpenPGP-software til at dekryptere e-mailen og læse indholdet.

Brug en dedikeret sikker e-mail-udbyder
Hvis du ikke ønsker at gå igennem besværet med manuelt at aktivere S/MIME eller OpenPGP-kryptering på din traditionelle webbaserede e-mail-konto, er en meget nemmere måde at sende en sikker e-mail på at oprette en konto hos en sikker e-mail-udbyder.

Med en sikker e-mail-udbyder som ProtonMail, vil du være i stand til at sende sikre, krypterede e-mails til andre, uanset om de bruger den samme sikre e-mail-udbyder, som du bruger, og din(e)

modtager(e) vil også være i stand til at svare sikkert. Mange sikre e-mail-udbydere implementerer OpenPGP-kryptering for at sikre brugernes e-mails og vil tillade brugere nemt at sende og modtage sikre, krypterede e-mails med andre, der har OpenPGP-kryptering aktiveret med deres e-mail-klienter. Hvis din modtager ikke har PGP aktiveret, vil du stadig være i stand til at sende en e-mail sikkert til den pågældende modtager, som kun kan åbnes ved hjælp af en delt hemmelighed.

Dybest set, når du bruger en sikker e -mail- udbyder , vil du nemt være i stand til at beskytte følsomme meddelelser ved at kryptere dem, alt sammen på en platform, der typisk er lige så enkel at bruge som de store e-mail-udbydere som Gmail, Yahoo! eller Outlook. Men i modsætning til disse store navneudbydere vil en sikker e-mail-udbyder ikke irritere dig med reklamer eller overvåge dine e-mails (da den ikke engang kan få adgang til dem takket være ende-til-ende-kryptering).

Ulempen er, at du skal betale for at få adgang til en sikker e-mail-udbyders fulde liste af funktioner, udvidet lagerplads og ubegrænsede meddelelser. Mange af de bedste sikre e-mail-udbydere tilbyder dog et gratis niveau (med visse begrænsninger), der giver dig mulighed for at sende og modtage sikre e-mails gratis. Hvis du kun skal sende et begrænset antal sikre e-mails, så kunne en gratis mulighed bestemt være en levedygtig løsning, men hvis du planlægger at udføre størstedelen af din e-mail-korrespondance på en sikker måde, så køb en præmie abonnement vil være nødvendigt.

Når du modtager en e-mail, skal du være opmærksom på

- afsenderens identitet er ikke garanteret: den kontrollerer forholdet mellem afsenderen og indholdet af meddelelsen;
- Åbn ikke vedhæftede filer, der kommer fra ukendte personer eller er forbundet med legitime konti, men med beskeder med mistænkeligt emne og indhold. De kan indeholde ondsindet software (ondsindet software eller malware, såsom orme, trojanske heste, spyware, former for adware osv.);
- hvis det er absolut nødvendigt at åbne en vedhæftet fil, selv fra legitime e-mails, skal den først downloades og scannes med den installerede antivirusløsning og derefter åbnes med den tilhørende applikation;
- i tilfælde af e-mails, der indeholder links, skal du ikke få direkte adgang til dette link i meddelelsens brødtekst; det link kan muligvis kopieres og åbnes fra en anden browserfane;
- ikke besvare e-mails, der indeholder anmodninger om personlige eller fortrolige data (f.eks . PIN-kode og bankkortnummer).

Hvordan ved du, at din e-mail blev "tilganget" af ukendte personer?

- dine kontakter siger, at de har modtaget spam-e-mails fra dig;
- du modtager mange e-mails med fejl;
- beskeder vises i mappen "sendte", uden at du sender dem;
- Kontoens placeringshistorik i login-handlingen svarer ikke til din aktuelle aktivitet.

Adgangskodesikkerhed. Angrebene har til formål at identificere adgangskoden og få adgang til de oplysninger, der er begrænset af denne adgangskode. De mest anvendte angrebsmetoder af denne type er "ordbogsangreb" og "brute force".

"Ordbogsangreb" sigter mod uautoriseret adgang til nogle ressourcer eller computersystemer ved successivt at prøve de adgangskoder/dekrypteringsnøgler, der findes i en foruddefineret liste af ord eller sætninger.

Et "brute force"-angreb er en metode til uautoriseret adgang til et computersystem eller til at afkode krypteret indhold (såsom adgangskoder) ved hjælp af "brute force"-beregning - gennem programmer, der anvender trial-error-metoden. Metoden består i successivt at prøve alle mulige kombinationer af tegn, uden en omfattende algoritme.

Foranstaltninger: captcha-system, adgangstiming efter en række mislykkede adgange.

- bruge unikke ID'er og adgangskoder og ikke kommunikere dem til andre brugere;
- Længden af adgangskoden og dens kompleksitet skal vælges, så den er svær at gætte, men nem at huske;
- periodisk ændring af adgangskoder (med et interval på 1-3 måneder);
- brug af forskellige adgangskoder til forskellige applikationer;
- brugen af flere autentificeringsmetoder (PIN, fingeraftryk, advarselsmeddelelser osv.);
- undgå at bruge lignende adgangskoder i hjemmet og på arbejdet.

Brug ikke:

- navnet på dig, en anden i familien eller dit yndlingsdyr ,
- elementer i din adresse: bygningens navn, gade, land,

- navnet på institutionen, projektet osv.,
- telefonnummer, registreringsnummer
- navnet på yndlingsstjernen eller -karakteren (eller på filmen, bogen osv.)
- ordbogsord;
- navnet på den konto, som du har angivet adgangskoden til;

Metoder, der giver en falsk følelse af stærke adgangskoder

- fonetisk metode: "Jeg ved med sikkerhed, at jeg har en Blu-Ray DVD!": St1u100%km1DVDBLr!
- første bogstavsmetode: "Jeg ved med sikkerhed, at jeg har en Blu-Ray DVD!": "sSka1DVDBr!"
- substitutionsmetode (normalt vokaler): Erstat visse bogstaver med talsymboler i et ord. Skift f.eks. æble til @3bl3.
- omvendt og substitutionsmetode: "Jeg elsker ferier": "r0d@3l11d3cn0c"
- store/små bogstaver, tal/symbol og erstatningsmetode: "Jeg elsker ferier": "@D0 rC)nC 3d11L3"
- tilpasning af metoder i henhold til websteder for at skabe et personligt adgangskodegenereringssystem: Gmail - "G@D0 rC)nC 3d!1L3MAIL", Yahoo - "YA@D0rC)nC3d!1L3HOO", Wizzair - "WIZZ@D0rC) nC3d!1L3AIR".

Brug ikke disse metoder! Mens de engang repræsenterede normen, gjorde CPU-kraft dem for det meste irrelevante. Nutidens adgangskodeknækningsværktøjer reducerer effektiviteten af de tidligere nævnte metoder.

En bedre måde at oprette adgangskoder på er at bruge hele sætninger, mens du inkluderer store bogstaver, små bogstaver, tal og helst specialtegn. På den måde kræver automatiserede scripts, der nemt bruger arkaiske metoder, som de diskuterede, en enorm indsats for at brute force eller gætte dit kodeord. Den nye metode kaldes "adgangssætninger", og den kan nå op til 100 tegn eller mere.

Adgangssætningen anses for at være overlegen i forhold til adgangskoden, fordi den er lettere at huske og sværere at hacke. Det er lettere at huske en tilfældig sætning med 4 til 8 ord i stedet for en kompleks streng af bogstaver, tal og specialtegn på 30 tegn. Selv de mest avancerede værktøjer til krakning af adgangskode er ikke i stand til at brute force en adgangssætning, der bruger tilfældige ord og er af betydelig længde.

Sådan opretter du en adgangssætning

• Kombiner en gruppe ord til en sætning, der giver mening for dig, men ikke for andre

• Brug ikke almindelige sætninger eller berømte citater

• Tilføj mellemrum inden for og mellem ordene

• Brug store bogstaver og brug nogle af ordene med stort

• Tilføj tegnsætning og specialtegn, der giver mening for dig

• Brug usædvanlige stavemåder af ord

En anden måde at udvikle en adgangssætning på er at linke til en personlig historie eller privat hukommelse. Nøgleord kan bruges til at fortælle historien.

Samlet i dette enhedsmodul

Sådan bruges Cyber Kill Chain effektivt i din cybersikkerhedsstrategi

Opdag – Analyser og find indtrængensforsøgene.

Afvis – Stop angrebene, efterhånden som de sker.

Afbryde – Stop datakommunikationen

Nedbryde – Reducer og begræns effektiviteten af angrebet.

Bedrag – Led angriberne i den forkerte retning.

Indeholder – Skjul og begræns angrebets rækkevidde, så det kun påvirker en del af organisationen.

Spørgsmål:

Spørgsmål Diskussionsforum skal besvares med en kort forklaring. Svarene vil blive drøftet med mentoren under mentorsessionerne

- Hvad er malware
- Hvilke er de vigtigste cybertrusler
- Hvilket er rollen for Secure Web Server - SSL

- Forklar nogle regler for sikrere browsing
- Præsenter nogle foranstaltninger til at sikre afsendelse og modtagelse af e-mail

Selvevalueringsspørgsmål. Efter besvarelsen kan eleven se resultaterne og sammenligne dem med disse gemt på platformen

- Malware
- De vigtigste cybertrusler
- Regler for sikrere browsing
- Foranstaltninger til at sikre afsendelse og modtagelse af e-mail

Vedhæftede filer (PowerPoint-præsentation, uddelingskopier, udskrifter, links, video...):

Se Powerpoint- og videofiler

Referencer:

- Hvad er Cybersikkerhed?

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

- Malware eller skadelig software

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

- Cybersikkerhed for alle.

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

- Software til fjernelse af malware 2022; Sikre dine personlige data

URL: Malware

- Hvad er cybersikkerhedstrusler?

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

- 21 Top cybersikkerhedstrusler og hvordan trusselsintelligens kan hjælpe

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

- Afsendelse og modtagelse af e-mail

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

- Opret og send e-mail

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

Cyber Kill Chain: De syv trin i et cyberangreb

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