SYSTEM GRUPPEN
- din eksterne IT afdeling

IT-SIKKERHED

Praktiske Råd til hvordan du forbedrer din sikkerhed i dag

Praktiske Råd

Nedenfor følger praktiske råd til, hvordan man umiddelbart kan forbedre sin IT-sikkerhed ved at tage fat i såkaldte "lavt hængende frugter". Det anbefales dog, at man tager fat i de 20 CIS Controls og anbefalingerne deri – i særdeleshed de fem første – da disse tilbyder en mere omfattende beskyttelse.

Tilslut kun USB-nøgler og harddiske, du har kendskab til.

Fysiske enheder kan blive ramt af malware gennem mange kanaler – ikke kun gennem internettet. Cyber-kriminelle kan have inficeret USB-nøgler og harddiske med malware med formålet at ramme det udsete offer. Derfor skal man kun tilslutte eksterne enheder, som man har kendskab til, og hvis man kender kilden.

Verizon's Chris Novak foreslå, at man skal tænke på USB-nøgler som tandbørster, hvorfor man bør være tilbageholdende, når det kommer til at dele dem og bruge andres.

Forlad ikke dine enheder ulåste og uden opsyn

I samme åndedrag som ovenstående frarådes det, at man efterlader sine enheder ulåste og uden opsyn. Ligesom man ikke efterlader sin bil ulåst med nøglen i, bør man heller ikke med sine enheder, da de cyber-kriminelle derved får let adgang til dine oplysninger og data samt muligheden for at kompromittere enheden.

Vær påpasselig og opmærksom på, hvilken software du installerer

Dette kan virke åbenlyst, men nogle brugere bliver kompromitteret med malware gennem inficeret software. Derfor skal man være forsigt ig med hvilke software, man installerer, og man bør ikke installere og køre software, der er downloadet fra internettet – hvis sådan en handling er tilladt i virksomheden – medmindre softwaren er hentet fra en troværdig kilde eller er blevet scannet for malware. Man bør altid hente softwaren fra udbyderens officielle webside. Derudover bør man ikke hente piratkopier, både af juridiske grunde men også fordi disse ofte er inficeret med malware.

Husk Firewall

Installér en hardware baseret firewall i virksomheden for at sikre perimeteren af netværket. Sørg for at lukke alle porte ind mod netværket. Servere, der skal publiceres, bør placeres i en DMZ zone, så de er adskilt fra det interne netværk, og kun de nødvendige porte bør åbnes ind mod serverne i DMZ zonen. Udvælg hvilke porte brugerne må benytte til udgående kommunikation, og luk derefter resten. Dermed lukkes der for f.eks. en inficeret PC der forsøger at sende mails ud direkte på port 25, eller en bruger der forsøger at downloade piratkopier via en

torrent webside, der benytter peer-to-peer trafik. Udskift den gamle firewall med en model der understøtter intrusion detection og prevention, samt deep packet inspection. Disse værktøjer kræver typisk ekstra licenser til firewall'en, men når de er aktiveret, undersøger de ind- og udgående pakker for ondsindede malware, og blokerer det herefter.

Husk også at have Windows Firewall eller en firewall fra et anti-virus program aktiveret på alle computere og servere. Det nedsætter risikoen for at en computer bliver udnyttet af en hacker. Mange slukker for firewallen fordi det er besværligt at opsætte, men det udgør en stor trussel at slukke firewallen på computere og servere.

Vær aggressiv i opdatering af din software

Det er vigtigt at opdatere og patche sin software og styresystem for at lukke sårbarheder, som de cyber-kriminelle kan udnytte. Derfor bør man være aggressiv i at opdatere sit styresystem og sin software i den forstand, at når der kommer en ny opdatering, så installerer man den. Og når det er muligt, så bør man automatisere opdaterings-processen.

Anvend anti-virus software

Endnu et råd der ligger til højrebenet. Sørg for at have et robust anti-virus og –malware system, der kan beskytte dit miljø mod malware.

Husk at sætte programmet til at scanne dine systemer regelmæssigt, hvilket kan gøres manuelt eller automatisk ud fra et specificeret tidsinterval.

Fjern administrator-privilegier

Når man er har administrator-privilegier, må man alt på computeren. Der vil sige: Installere programmer, installere drivere, ændre firewall-opsætning, og alt andet. Hvis sådan en bruger bliver inficeret gennem sårbarheder, der tillader, at den cyber-kriminelle har samme privilegier som den bruger, der er logget ind, så har den cyber-kriminelle fuld adgang. Men hvis man fjerner administrator-privilegierne, så fjerner man ikke sårbarhederne, men man reducere kraftigt den skade, de kan medføre.

Begræns brugerrettigheder

Gennem en begrænsning af brugerrettigheder sikrer man sig, at hvis en bruger skulle blive inficeret af ondsindet kode og malware, så har bagmændene kun adgang til en begrænset mængde data og rettigheder. Således begrænses omfanget og indvirkningen af angrebet.

Hver bruger bør indstilles således, at personen akkurat kan udføre sit arbejde med mindst mulige brugerrettigheder.

Følg "Best Practice" når det kommer til adgangskoder

Første aspekt, man bør kigge på, når man skal sikre sine adgangskoder, er at implementerer 2-faktor login, hvor man skal logge ind med både adgangskode og SMS-kode eller biometri.

Kigges der på selve adgangskoden, skal man sikrer sig, at man bruger stærke adgangskoder. En stærk adgangskode består af minimum otte tegn, der består af måde numre og tegn, der skal være både store og små. Til formålet kan der anvendes passphrases.

Derudover bør adgangskoden skiftes hver tredje måned, og den samme adgangskode bør aldrig bruges to gange. Dette kan gennemtvinges for brugerene i et domæne med Group Policy eller Fine-Grained password policies.

Man bør også have forskellige kodeord til hver konto (f.eks. e-mail), software og login man har. Til formålet at huske alle de forskellige, foranderlige adgangskoder kan en password manager tages i brug.

Generér logs

Få dit system til at genererer logs på alt, der foretages, da disse kan bruges til at identificere problemer og årsager hertil, hvis der bliver brug for det.

Alle logs bør opsamles i en syslog server, hvorfra det er muligt at opsætte triggers på forskellige events fra logfilerne, som viser tegn på en hacker er inde i systemet eller forsøger på at komme ind.

Anvend et effektivt spamfilter

Med mere end 100 mia. spam e-mails om dagen på global plan, som kan være inficeret med malware, er det vigtigt at kunne frafiltrerer denne uønskede post. Denne rolle påtager spamfilteret sig, således at trusselsaktørernes e-mails har mindre chance for at nå medarbejderne og for at inficere virksomhedens system.

Implementér browser beskyttelse

Den af de cyber-kriminelle anden mest brugte leveringskanal for malware er internetbaserede drive-by angreb. Derfor bør virksomheden opsætte browser beskyttelse – f.eks. gennem et add-on til anti-virus programmet – for at forhindre de web-baserede angreb.

En anden måde at sikre sig på internettet er ved at implementerer et såkaldt "URL reputation plugin", som fremviser den specifikke websides anseelse/omdømme ved søgninger.

Aktivér "Filtypenavne"-muligheden

De cyber-kriminelle prøver i nogle tilfælde at skjule deres skadelige malware ved at kalde dem for et andet format (f.eks. xxx.pdf.exe eller xxx.doc.scr). Hvis ikke ”Filtypenavne”-muligheden er slået til vil den tilsendte fil ligne en troværdig fil i et troværdigt format (xxx.pdf eller xxx.doc). Men dette problem kan altså løses ret simpelt ved at slå ”Filtypenavne”-muligheden til, hvorefter man vil kunne identificere den rigtige filtype.

Slå automatisk eksekvering af makro'er fra

Trusselsaktørerne kan anvende sårbarheder i Microsofts Officepakke gennem makro'er. Derfor rådes man til at slå den automatiske eksekvering af disse fra (hvis dette ikke allerede er gjort), hvorved risikoen for inficering reduceres.

Backup! Backup! Backup!

Eftersom man som virksomhed ikke kan opnå absolut beskyttelse mod alle cyber-sikkerhedstrusler, så er det vigtigt, at man har en backup. Hvis virksomheden rammes af eksempelvis ransomware eller anden malware, er det essentielt for virksomhedens evne til komme tilbage til normal drift, at der findes en backup og således sikre, at virksomhedens data ikke er ødelagt og mistet for evigt.

Det bedste er at have to backups, en i skyen som sikre mod bl.a. oversvømmelse, brand og lynnedslag, og en der kan gemmes i nærheden af serverne som kan bruges til hurtig restore af data i tilfælde af sletning eller hacker angreb. Samtidigt skal backupsene tjekkes med jævne mellemrum. Skemalæg test-restore af alle backupsene for at sikre integriteten af dataene.

Stol ikke på nogen. Bogstaveligt talt.

Vær påpasselig med at åbne vedhæftede filer og links, når du modtager e-mails eller andre former for beskeder, da cyber-kriminelle ofte distribuerer falske e-mails – og såkaldte phising e-mails – for at få fat i folks følsomme oplysninger og for at få dem til at installere malware på deres enhed..

Selv når vedhæftningerne kommer fra troværdige kilder og venner skal man forholde sig med sin sunde fornuft, da enhver konto kan blive kompromitteret.

Undervis medarbejderne i sikker adfærd på de sociale medier

I takt med at social engineering er blevet en større og større del af de cyber-kriminelles arsenal, så er vores adfærd på de sociale medier blevet yderst relevant. Trusselsaktørerne leder aktivt efter information, de kan bruge til at udnytte i angreb og i phising og spear-phising e-mails.

Derfor bør man passe på med, hvad man deler online. Derudover skal man også passe på, og for det meste helt lade være med at acceptere ukendte venneanmodninger på de sociale medier. Dertil skal man også være opmærksom på, at de links til tilbud, der virker alt for gode, også oftest er det, at ikke alle link føre til ægte login-sider, og aktuelle emner og begivenheder er det mest brugte lokkemad for svindlere.

Cyber-sikkerhed er alles ansvar

Når det kommer til cyber-sikkerhed, er man ikke stærkere end sit svageste link. Derfor skal alle medarbejdere tage ansvar for cyber-sikkerheden og undervises i, hvad der er acceptabelt.

Selvom man i virksomheden har anti-virus programmer og andet sikkerhedssoftware, så er det ikke i orden at besøge ondsindede og tvivlsomme hjemmesider.

Derudover bør medarbejderne opfordres til at slå alarm, hvis de opdager noget mistænksomt, således angrebet fra de cyber-kriminelle kan begrænses og håndteres.

Vær påpasselige med dine fortrolige oplysninger

Generelt set bør man være påpasselig med hvem og på hvilke sider, man giver sine fortrolige data, da de cyber-kriminelle sælger og udnytter dette.

HTTPS er mere sikkert

I modsætning til ”http”, så er ”https” en krypteret måde at kommunikerer på internettet. Derfor bør man, når man videregiver sine personlige og følsomme oplysninger holde øje med, om den pågældende hjemmeside kommunikerer gennem ”https”.

Deaktivér automatisk afspilning via. Flash

Flash objekter er nogle af de mest normale at finde på ondsindede sider, da Flash har en masse sårbarheder. Derfor er det en god idé at deaktivere den automatiske afspilning af Flash objekter, og derved reducere risikoen for at blive inficeret.

Brug en VPN forbindelse på offentlige netværk

Offentlige netværk (f.eks. dem i hoteller, caféer og lufthavne) er ikke ret sikre, da de deles af en stor mængde af mennesker samtidigt, hvilket betyder, at dine data potentielt set er i fare.

For at sikre sig på et offentligt netværk anbefales det derfor, at man anvender en VPN forbindelse. Sådan en forbindelse sikrer, at al din aktivitet sker gennem separate, sikre og privat netværk. Det sker bl.a. ved, at din trafik bliver krypteret, en sikkerheds-tunnel skabes til internettet og fil-deling bliver deaktiveret,

hvilket gør dig langt mindre udsat for angreb og beskytter dine følsomme data.

Husk mobil-sikkerhed

En af tendenserne for 2016 var at mobile enheder i højere grad blev ramt af malware, derfor er det vigtigt også at være beskyttet på denne front.

Man bør sikrer sig, at man har muligheden for at slette sin data automatisk, hvis enheden bliver stjålet. Derudover bør man begrænse den tid, hvori ens enhed er ulåst, når den ikke anvendes, og bruge en stærkere adgangskode end blot fire cifre. Slutteligt skal man også være påpasselig med at installere gratis applikationer til Android-enheder, da der findes mange tvivlsomme applikationer.

Hav en beredskabsplan

For at sikre at man kan reagere hurtigt, hvis man bliver inficeret, er det en god idé at have en beredskabsplan klar. Det indebære, at man har kontaktinformationerne på den virksomhed, der står for virksomhedens IT-sikkerhed, at man ved hvem, man skal ringe til, og hvilke handlinger man skal udføre. Derudover skal man have en backup-og-restore-løsning klar og vide hvor ens backup befinder sig.

Hvis man bliver inficeret

I tilfælde af at man bliver inficeret og opdager en ondsindet eller ukendt proces på sin maskine, skal man med det samme frakoble den netværket og internettet. Dette vil forhindre infektionen i at brede sig. De(n) inficerede enhed(er)/netværk service skal altså isoleres, hvorefter problemet kan løses – enten gennem en backup-løsning eller indtil servicen er blevet patch-opdateret.

SYSTEM GRUPPEN

- din eksterne IT afdeling

www.systemgruppen.dk

mail@systemgruppen.dk

+45 96 45 55 00

Indkildevej 6F
9210 Aalborg SØ

@SystemGruppen

@SystemGruppen