OUCH! | Oktober 2017

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- Overblik
- Fem enkle trin
- Sådan sikrer du dine børn når de besøger andre

Sådan hjælper du andre med IT-sikkerhed

Overblik

Mange af os føler sig trygge ved at bruge teknologi og ved, hvordan vi bruger det på en sikker måde i vores hverdag. Vi har dog alle venner eller familiemedlemmer, der ikke er så trygge ved at benytte sig af det. Faktisk kan de være forvirrede, intimiderede eller endda bange for teknologien. Dette gør dem meget sårbare over for IT-angreb. IT-sikkerhed behøver ikke at være skræmmende, det er faktisk ret simpelt, når man forstår det grundlæggende. De fleste har sandsynligvis bare brug for en som dig til at hjælpe dem med at forstå det grundlæggende.

Gæsteredaktør

Randy Marchany (Twitter: **@randymarchany**) er CISO hos Virginia Tech og en certificeret SANS Institute instruktør.

Fem enkle trin

Her er fem enkle trin, du kan tage for at hjælpe andre med at overvinde deres frygt og få det bedste ud af dagens teknologi på en sikker måde. For mere information om hvert af disse punkter, se afsnittet ”Hvis du vil vide mere” i slutningen af dette nyhedsbrev.

1. **Social Engineering**: Social engineering bruges ofte af IT-kriminelle til at narre folk til at gøre noget, de ikke bør gøre, såsom at dele deres adgangskode, inficere deres computer eller dele følsomme oplysninger. Dette er ikke noget nyt, svindlere har eksisteret i tusindvis af år. Den eneste forskel er, at kriminelle nu anvender de samme teknikker på internettet. Du kan hjælpe andre ved at forklare dem, hvordan man genkender et sociale engineering angreb. Det er når du får en besked og afsenderen forklarer at det haster og er meget vigtigt, når noget er for godt til at være sandt, eller når du får en besked fra en du kender, men beskeden lyder anderledes end den plejer. Det kan i alle tilfældene være en IT-kriminel, der foregiver at være en anden. Del eksempler på almindelige social engineering angreb, som phishing-e-mails eller de berygtede Microsoft-telefonopkald. Du skal sørge for, at familie og venner forstår, at de aldrig bør give deres adgangskode til nogen eller tillade fjernadgang til deres computer.
2. **Adgangskoder**: Stærke adgangskoder er nøglen til at beskytte både dine enheder og eventuelle online-konti. Forklar din familie og venner, hvordan de opretter stærke adgangskoder. Vi anbefaler passphrases, da de er nemmeste at skrive og huske. Passphrases er intet andet end adgangskoder, der består af flere ord. Hjælp dem også med at installere

Sådan hjælper du andre med IT-sikkerhed

og bruge en password manager. Det er vigtigt at have et unikt kodeord til hver af dine enheder og konti. Hvis en password manager er overvældende, kan du måske lære dem at skrive deres adgangskoder ned og gemme disse adgangskoder på et sikkert sted. Endelig skal du hjælpe dem med at oprette to-trins bekræftelse til deres vigtigste konti (ofte kaldet to-faktor-godkendelse). To-trins bekræftelse er et af de mest effektive skridt, du kan tage for at sikre enhver konto.

Hjælp andre med at få det bedste ud af teknologien på en sikker måde ved at dele disse fem enkle trin med dem.

3. **Patching**: At holde sine systemer opdaterede er et vigtigt skridt, som alle kan tage for at sikre deres enheder. Dette gælder ikke kun dine computere og mobile enheder, men alt, hvad der er forbundet med internettet, såsom spilkonsoller, termometre eller endda lamper eller højttalere. Den enkleste måde at sikre, at alle enheder er opdaterede, er at slå automatisk opdatering til, på de enheder hvor det er muligt.
4. **Anti-Virus**: Folk begår fejl, sommetider klikker vi på links vi ikke bør klikke på eller installerer ting, vi sandsynligvis ikke burde have installeret. Dette kan inficere vores systemer. Anti-virus er designet til at beskytte os mod disse fejl. Anti-virus kan ikke stoppe alt malware, men hjælper ved at registrere og stoppe de mest almindelige angreb. Sørg derfor for, at alle hjemmecomputere har anti-virus installeret, og at det er opdateret og aktivt. Derudover omfatter mange af dagens anti-virusløsninger anden sikkerhedsteknologi som firewalls og browserbeskyttelse.
5. **Sikkerhedskopiering**: Hvis du er kommet til at slette de forkerte filer eller har været udsat for et IT-angreb, kan du gendanne dine filer fra backup. Sørg for, at familie og venner har et automatisk sikkerhedskopieringssystem. Ofte er de enkleste løsninger Cloud-baserede, disse kan lave backup af dine enheder hver time, eller når du ændrer en fil. Disse løsninger gør det nemt ikke kun at sikkerhedskopiere data, men også at genoprette dine filer.

Sådan sikrer du dine børn når de besøger andre

Hvis du er fortrolig med teknologien, har du sandsynligvis ikke kun sikret dig selv, men også dine børn. Men når børnene besøger en, der ikke er fortrolig med teknologien er disse venner eller slægtninge måske ikke opmærksomme på, hvordan man bedst kan beskytte børn online eller hvilke forventninger du har. Her er nogle trin, du kan tage for at beskytte børnene, når de besøger andre, især familie.

- **Regler**: Vær sikker på at dem, dine børn besøger, kender dine regler og forventninger til dine børns IT-sikkerhed.

Sådan hjælper du andre med IT-sikkerhed

Er der for eksempel regler om, hvor længe børn kan være online, hvem de kan tale med eller hvilke spil de kan eller ikke kan spille? Du skal ikke regne med, at dine børn forklarer reglerne til andre. En ide er at lave et 'regelsæt' og dele det med eventuelle familiemedlemmer og venner, dit barn ofte besøger.

- **Kontrol**: Hvis et barn forstår teknologien bedre end dem de besøger, kan de udnytte det. For eksempel kan børn anmode om eller få administrative rettigheder til en bedsteforældres computer og derefter gøre hvad de vil, såsom at installere det spil, du ikke vil have, at de spiller. Sørg for at familiemedlemmer forstår det og ikke giver børnene adgang.

Endelig kan du foreslå folk, at de abonnerer på ressourcer som OUCH! nyhedsbrev, så de kan fortsætte med at lære på egen hånd. Dette nyhedsbrev udgives hver måned gratis på over 20 sprog. Tilmeld dig på https://securingthehuman.sans.org/ouch.

Hvis du vil vide mere

På securingthehuman.sans.org/ouch/archives kan du tilmelde dig det månedlige nyhedsbrev om IT-sikkerhed fra OUCH! Her kan du ligeledes få adgang til ældre udgaver af OUCH! og læse mere om SANS IT-sikkerhedsløsninger

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Tidligere udgivelser

Social engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Password Manager:	https://securingthehuman.sans.org/ouch/2017#september2017
To-trinsbekræftelse:	https://securingthehuman.sans.org/ouch/2015#september2015
Backup og gendannelse:	https://securingthehuman.sans.org/ouch/2017#august2017
Sådan sikrer du dig dine børn når de er online:	https://securingthehuman.sans.org/ouch/2017#may2017

Licensinformation

Redaktion: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity

