OUCH! | August 2016

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- Hvad er ”ransomware”?
- Skal du betale løsesummen?
- Lav backup af dine filer
- Flere måder at beskytte sig på

Ransomware

Hvad er ”ransomware”?

Ransomware er en speciel type af ondsindet software (malware), som spreder sig på Internettet lige nu og som truer med at ødelægge ofrets dokumenter og andre filer. Malware er software – et program til computeren – der bruges til at udføre ondsindede handlinger. Ransomware er bare et eksempel på en af mange typer malware. Ransomware er blevet meget almindeligt fordi, det er så profitabel for de kriminelle. Så snart ransomware inficerer din computer, krypterer den udvalgte filer eller måske endda hele disken. Du bliver låst ude af hele systemet eller kan ikke tilgå vigtige filer såsom dokumenter eller billeder. Malware fortæller dig, at den eneste måde du kan få adgang til dit system eller filer, er ved at betale de IT-kriminelle en løsesum (”Ransom” er det engelske ord for afpresning, og det er derfor det kaldes ransomware). Ofte skal løsesummen betales i en digital valuta, som for eksempel Bitcoin. Ransomware spredes ligesom mange andre typer af malware. Den mest almindelig måde er ved at sende ofrene ondsindede e-mails, hvor de IT-kriminelle narrer dig til at åbne et vedhæftet dokument eller til at klikke på et link, som fører til angriberens hjemmeside.

Gæsteredaktør

Lenny Zeltser arbejder med at sikre kundernes IT-systemer ved NCR Corp, desuden underviser han i malware for SANS Institute. Lenny kan findes på Twitter som **@lennyzeltser**, og han skriver en blog om sikkerhed på **zeltzer.com**.

Skal du betale løsesummen?

Det er et svært dilemma. Problemet er, at jo oftere folk betaler de IT-kriminelle, jo flere angreb vil de blive motiveret til at udføre. På den anden side kan det være din eneste måde at få adgang til dine filer. Men en advarsel. Der er ingen garanti for, at du får adgang til dine filer, selvom du betaler. De er kriminelle, og de forsøger måske slet ikke at dekryptere filerne, noget kan gå galt i processen, eller din computer kan blive ramt af yderligere malware.

Lav backup af dine filer

Den bedste måde at slippe ud af ransomware uden at skulle betale en løsesum er ved hjælp af backup. På denne

© SANS Institute 2016

Ransomware

måde kan du genskabe dine filer på en ren computer. Husk at ransomware kan slette eller kryptere din backup, hvis den kan tilgås fra din inficerede computer. Det er derfor vigtigt at gemme dine backup filer ved en anderkendt leverandør i Skyen eller på eksterne diske, der ikke altid er forbundet til dit system. En fejl, som mange folk laver, er at antage at backuppen virker uden at afprøve om den kan bruges til at genskabe filerne. Husk at periodisk afprøve om dine backups virker og at du kan genskabe dine filer, hvis du skulle blive ramt af ransomware. Backups er vigtige idet de også hjælper, hvis du ved et uheld kommer til slette nogle filer, eller at din harddisk går i stykker.

Ransomware er en type af malware der gør, at du ikke har adgang til dine filer ved, at den krypterer dem, når den inficerer din computer.

Flere måder at beskytte sig på

Du kan beskytte dig imod ransomware på samme måde som du beskytter dig imod andre typer af malware. Undgå at blive inficeret. Start med at sikre, at du har et opdateret anti-virus program fra en anderkendt leverandør. Disse programmer kaldes nogle gange for anti-malware programmer, og er lavet til at opdage og stoppe malware. De kan dog ikke stoppe eller fjerne alt ondsindet software. IT-kriminelle finder hele tiden på nyt innovativt og mere sofistikeret malware, der kan undgå opdagelse. På den anden sider sørger anti-virus leverandørerne hele tiden for, at opdatere deres produkter med nye metoder til at opdage malware. På mange måder er det et våbenkapløb, hvor begge sider forsøger at komme foran. Desværre er de IT-kriminelle oftest et skridt foran, og du er nød til at tage backup af dine filer samt gøre brug af disse yderligere tiltag for at beskytte dig selv:

- IT-kriminelle inficerer ofte computeren ved hjælp af sårbarheder i softwaren. Jo oftere du opdaterer din software, jo færre kendte sårbarheder har den og det bliver svære for de IT-kriminelle at inficere din computer. Du skal derfor sørge for, at dit operativsystem, applikationer og enheder er konfigureret til automatisk at installere opdateringer.
- Brug en almindelig bruger med få rettigheder på computeren i stedet for administrator eller root-brugeren. Dette forhindrer mange typer af malware i at blive installeret.

© SANS Institute 2016

Ransomware

- IT-kriminelle narrer ofte folk til at installere deres malware for dem. De kan sende dig en e-mail som indeholder et link eller en vedhæftet fil. E-mailen ser måske ud til at komme fra din bank eller en ven. Men når du klikker på linket eller åbner filen, startes det ondsindede software og malwaren installes. Ofte forsøger e-mailen at give indtryk af at det haster, er vigtigt, måske indeholder den et tilbud, som er for godt til at være sandt, eller måske er den dårligt skrevet. Vær skeptisk. Sund fornuft er dit bedste forsvar.

Beskyt dig selv imod ransomware ved at være skeptisk før du åbner vedhæftede filer eller før du klikker på links. Sørg for at din antivirus er opdateret, at der bliver taget backup af dine filer, og at du kan genskabe filerne fra dine backups.

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 og med 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 http://www.welcomesecurity.net.

Tidligere udgivelser (ikke oversat til dansk)

Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
What is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Encryption:	https://securingthehuman.sans.org/ouch/2016#june2016
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Microsoft Article:	https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS FOR610 Course - Reverse Engineering Malware:	https://sans.org/for610

Licensinformation

OUCH! er udgivet af SANS Securing The Human og distribueres under Creative Commons BY-NC-ND 3.0 licensen. Du er velkommen til at videregive dette nyhedsbrev eller bruge det i dit eget arbejde med IT-sikkerhed så længe du ikke ændrer i nyhedsbrevet. Hvis du har spørgsmål til oversættelsen eller andet er du velkommen til at kontakte ouch@securingthehuman.org.

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity