OUCH! | Juni 2017

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- Overblik
- Opdater
- Backup
- Phishing

Hvad kan vi lære af WannaCry?

Overblik

For nylig så du sandsynligvis en enorm nyhedsdækning af et nyt IT-angreb kaldet "WannaCry". "WannaCry" inficerede over 200.000 computere, og låste dermed en række organisationer ud af deres data, herunder hospitaler i Storbritannien. Der er flere grunde til, at dette angreb fik så meget opmærksomhed. For det første spredtes det hurtigt fra computer til computer ved at angribe en kendt svaghed i Windows-computere. For det andet var angrebet en type malware der kaldes "Ransomware". Dette betyder at hvis den inficerede din computer, ville den kryptere alle dine filer og dermed låse dig ude fra dine data. Den eneste måde, du kan gendanne dine data på, er fra backup eller ved at betale angriberen en løsesum på ca. 2000 kr. for at dekryptere alle dine data. Den tredje og vigtigste årsag er, at et angreb som dette burde aldrig have fundet sted. Den svaghed som "WannaCry" angreb i Windows-computere var velkendt af Microsoft, der havde frigivet en opdatering måneder tidligere. Men mange organisationer undlod at installere opdateringen eller anvendte operativsystemer som Windows XP, der er så gamle, at der ikke var nogen opdatering, der er tilgængelig. Her er tre enkle trin, du kan tage for at sikre, at angreb som "WannaCry" ikke rammer dig.

Gæsteredaktør

Dr. Johannes Ullrich er "Dean of Research" for SANS Technology Institute og grundlægger af DShield.org. Han er ansvarlig for SANS "**Internet Storm Center**", der overvåger aktuelle IT-sikkerhedstrusler. Han underviser i: "Web Application Security (**DEV522**)", "Intrusion Detection (**SEC503**)" og "IPv6 (**SEC546**)".

Opdater

Først og fremmest skal du sørge for, at dine computere, mobilenheder, apps og alt andet, der er forbundet med internettet, er opdateret. IT-kriminelle søger konstant efter nye sårbarheder i den software, dine enheder anvender. Når de opdager sårbarheder, bruger de specielle programmer til at hacke i de enheder, du bruger. I mellemtiden er de virksomheder, der skabte softwaren til dine enheder, på hårdt arbejde for at løse disse sårbarheder ved at frigive opdateringer. Ved at sikre, at dine computere og mobile enheder installerer disse opdateringer, gør du det meget sværere for nogen at hacke dig. Det er det, der er så frustrerende ved WannaCrys udbredelse. Opdateringerne til at rette og stoppe dette angreb var blevet frigivet næsten to måneder tidligere af Microsoft. Hvis organisationerne havde holdt deres computere opdateret, ville dette angreb aldrig have fungeret. For at sikre, at dine enheder forbliver opdateret, skal du aktivere

Hvad kan vi lære af WannaCry?

automatisk opdatering, når det er muligt. Denne regel gælder for næsten enhver teknologi, der er forbundet til et netværk, ikke kun dine computere og mobile enheder, men internetforbundne tv'er, routere, spillekonsoller eller en dag måske endda din bil. Hvis dine operativsystemer eller enheder er så gamle, at de ikke længere understøttes af sikkerhedsopdateringer, som f.eks. Windows XP, skal du erstatte dem med nye, der understøttes.

Nøglen til at beskytte dig mod angreb som WannaCry er tre enkle trin; Hold dine enheder opdateret, pas på phishing-angreb og lav sikkerhedskopier af dine systemer.

Backups

I nogle tilfælde kan IT-angreb som ransomware endda inficere opdaterede systemer. En måde at beskytte dig mod dette på er ved at sikkerhedskopiere dine data. Sikkerhedskopier er kopier af dine oplysninger der er gemt andetsteds end på din computer eller mobilenhed. Når du mister værdifulde data, kan du gendanne data fra dine sikkerhedskopier. Desværre undlader for mange mennesker at lave sikkerhedskopier regelmæssigt, selvom det er enkelt og billigt. Der er to måder at sikkerhedskopiere dine data på: fysiske medier eller skybaseret lagring. Hver tilgang har fordele og ulemper. Du kan bruge begge tilgange på samme tid, hvis du er usikker på hvilken metode du skal bruge.

Fysiske medier er enheder, du styrer, såsom eksterne USB-drev eller netværksforbundne drev, der findes i dit hjem eller kontor. Fordelen ved at bruge dine egne fysiske medier er, at de giver dig mulighed for at sikkerhedskopiere og gendanne store mængder data meget hurtigt. Ulempen ved en sådan tilgang er, at hvis du bliver inficeret med malware, som ransomware, er det muligt for infektionen at sprede sig til dine sikkerhedskopier. Hvis du bruger fysiske medier til sikkerhedskopiering, skal du gemme kopier af din backup på et sikkert sted som ikke er samme sted som enheden du har lavet backup af. Sørg for, at eventuelle sikkerhedskopier, du gemmer, er korrekt mærket. Sky-baserede løsninger er online-tjenester, der laver backup og gemmer dine filer på internettet. Normalt installerer du et program på din computer, der tager sig af alt. Fordele ved sky løsninger er deres enkelhed. Hvis du bliver smittet med ransomware, kan infektionen normalt ikke få adgang til dine sky-baserede sikkerhedskopier. Ulemperne er, at det kan tage lang tid at sikkerhedskopiere eller gendanne meget store mængder data. Sørg for at undersøge sikkerhed for skybackups samt hvordan leverandøren beskytter dit privatliv. Giver backup-tjenesten en stærk sikkerhed såsom kryptering af dine data og kræves der stærk brugergodkendelse, for eksempel to-faktor logon?

Hvad kan vi lære af WannaCry?

Phishing

De IT-kriminelle opdaterer og ændrer altid deres angrebsmetoder. Normalt bruger de en anden angrebsmetode, der kaldes phishing, til at angribe og inficere ofre. Phishing er, når IT-kriminelle sender dig en e-mail, der forsøger at narre dig til at åbne en inficeret vedhæftet fil eller besøge en ondsindet hjemmeside. Hvis du gør det, kan din computer blive smittet. “WannaCry” brugte ikke denne angrebsmetode, men den bruges ofte i mange andre typer angreb, herunder de fleste typer af ransomware. Derudover vil de IT-kriminelle, der udviklede WannaCry, uden tvivl opdatere deres angrebsmetoder i de kommende måneder og bruge nye teknikker som phishing til at inficere endnu flere computere. Nøglen til at beskytte dig mod sådanne e-mailbaserede angreb er sund fornuft. Hvis en e-mail eller en meddelelse virker underlig, mistænkelig eller for god til at være sandt, er det højst sandsynligt et angreb.

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

What is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Ransomware (oversat til dansk):	https://securingthehuman.sans.org/ouch/2016#august2016
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Using the Cloud Securely (oversat til dansk):	https://securingthehuman.sans.org/ouch/2016#november2016

Licensinformation

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

