OUCH! | Juni 2017

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Hva vi lærte av WannaCry

Oversikt

I det siste har du mest sannsynlig sett den enorme mediedekningen av cyberangrepet kalt "WannaCry". "WannaCry" infiserte over 200.000 datamaskiner og låste forskjellige organisasjoner ute fra dataene deres, inkludert sykehus i Storbritannia. Det er flere grunner til at dette angrepet fikk så mye oppmerksomhet. For det første spredte den seg hurtig fra datamaskin til datamaskin ved å utnytte en kjent sårbarhet i Windows-datamaskiner. For det andre var angrepet en type skadevare kjent som "løsepengevirus" (eller ransomware på engelsk), noe som betyr at når det infiserer datamaskinen, krypterer den alle filene dine, slik at du blir låst ute fra viktige data. Den eneste måten man kunne gjenopprette dataene var ved sikkerhetskopi, eller ved å betale angriperen i overkant av 2500 kr i løsepenger for å dekryptere filene. Det tredje og mest viktige er at dette angrepet aldri skulle skjedd. Sårbarheten "WannaCry" angrep i Windows-datamaskinene var godt kjent av Microsoft, som hadde utgitt en sikkerhetsoppdatering noen måneder i forveien. Men mange organisasjoner gjorde den feilen å ikke installere sikkerhetsoppdateringen, eller brukte fremdeles operativsystemer som Windows XP, som er så gamle at det ikke er noen sikkerhetsoppdatering tilgjengelig lenger. Her er tre enkle steg du kan ta i bruk for å sørge for at angrep som "WannaCry" aldri infiserer deg.

Gjesteredaktør

Dr. Johannes Ullrich er Dean of Research ved SANS' teknologiske institutt, og grunnlegger for DShield.org. Han er ansvarlig for **SANS Internet Storm Center** hvor aktive trusler mot cybersikkerheten overvåkes. Han lærer bort sikkerhet i web-applikasjoner (**DEV522**), intrusion detection (**SEC503**) og IPv6 (**SEC546**).

Oppdatering

Først og fremst bør du sørge for at alt du har av datamaskiner, mobile enheter, apper og alt annet som er på nett, er oppdatert. Cyberkriminelle leter hele tiden etter sårbarheter i programvaren som kjører på enhetene dine. Når de oppdager sårbarheter, bruker de spesiallagde programmer for å hacke seg inn på enhetene dine. I mellomtiden jobber selskapene som har laget programvaren på enhetene dine hardt for å få fikset disse svakhetene, ved å gi ut oppdateringer. Ved å sørge for at det du har av datamaskiner og mobile enheter får disse oppdateringene, gjør du det mye vanskeligere for noen å hacke deg. Det er det som er frustrerende ved spredningen av WannaCry. Oppdateringene som kunne stoppet dette angrepet ble sluppet nesten to måneder i forveien av Microsoft. Om alle organisasjonene hadde holdt datamaskinene sine oppdatert, ville

Hva vi lærte av WannaCry

angrepet aldri ha fungert. For å sørge for at enhetene dine holder seg på nyeste versjon, bør du aktivere automatiske oppdateringer hvor enn det er mulig. Denne regelen gjelder for så å si all teknologi som er koblet til et nettverk, ikke bare datamaskiner og mobile enheter, men også TV-er med internettilkobling, hjemmeroutere, spillkonsoller, og kanskje til og med bilen din. Dersom operativsystemet på enhetene er såpass gammelt at det ikke lenger er støttet med sikkerhetsoppdateringer, slik som Windows XP, må du bytte dem med nye som er støttet.

Nøkkelen til å beskytte seg selv mot angrep som WannaCry er tre enkle grep: Hold datamaskinene oppdaterte, vær på vakt overfor phishing-angrep, og ta sikkerhetskopi av systemet.

Sikkerhetskopiering

I noen tilfeller kan angrep med løsepengevirus til og med infisere datasystemer som mer fullt oppdaterte. Et ekstra tiltak for å beskytte seg selv er å ta sikkerhetskopi av dataene dine. Sikkerhetskopier er kopier av informasjonen din som er lagret på et annet sted enn på datamaskinen din eller mobilen din. Når du mister verdifull data, kan du gjenopprette den dataen fra en sikkerhetskopi. Dessverre er det alt for mange folk som ikke tar jevnlig sikkerhetskopi, selv om det er enkelt og billig. Det finnes to metoder for sikkerhetskopiering: Fysiske lagringsmedier, eller sky-basert lagring. Hver tilnærming har fordeler og ulemper. Dersom du er usikker kan du bruke begge to samtidig.

Fysiske lagringsmedier er enheter du kontrollerer selv, som eksterne USB-disker, eller nettverks-lagringssystemer basert i hjemmet ditt eller på kontoret. Fordelen med å bruke dine egne fysiske lagringsmedier er at det lar deg ta sikkerhetskopi og gjenopprette store mengder data veldig fort. Ulempen med en slik tilnærming er at dersom du blir infisert med skadevare, som løsepengevirus, kan det muligens spre seg til sikkerhetskopiene dine. Dersom du bruker fysiske lagringsmedier for sikkerhetskopi burde du lagre kopier av sikkerhetskopien på et fysisk adskilt, trygt sted. Sørg for at alle sikkerhetskopier du lagrer er skikkelig merket. Sky-baserte løsninger er tjenester på nett som tar sikkerhetskopi av filene dine og lagrer dem i nettskyen. Vanligvis installerer du bare et program på datamaskinen din som tar seg av alt. Fordelen med sky-baserte løsninger er at det er enkelt. I tillegg, skulle du bli infisert med løsepengevirus, kan det vanligvis ikke spre seg til dine sky-lagrede sikkerhetskopier. Ulempen er at det kan ta lang tid å sikkerhetskopiere eller gjenopprette store mengder data. Sørg også for å undersøke personvernet og sikkerheten til sky-løsningen. Tilbyr sky-leverandøren sterk sikkerhet som kryptering av filene dine, og skikkelig autentisering?

Hva vi lærte av WannaCry

Phishing

Til slutt, husk at de kriminelle alltid fornyer seg og endrer på angrepsmetodene sine. Cyberkriminelle bruker ofte en annen angrepsmetode kalt phishing for å angripe og infisere ofrene sine. Phishing er når cyberkriminelle sender deg en e-post og forsøker å lure deg til å åpne et infisert vedlegg eller besøke en skadelig nettside. Hvis du gjør noe av dette kan datamaskinen din bli infisert. Selv om "WannaCry" ikke brukte denne angrepsmetoden, er det vanlig med mange andre angrep, inkludert de fleste typer løsepengevirus. I tillegg vil de kriminelle som står bak WannaCry utvilsomt oppdatere angrepsmetodene sine i de kommende månedene, og bruke teknikker som phishing for å infisere enda flere maskiner. Nøkkelen til å beskytte seg selv mot slike e-postbaserte angrep er sunn fornuft. Dersom en melding eller henvendelse virker merkelig, mistenkelig, eller for god til å være sann, er det sannsynligvis et angrepsforsøk.

Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på securingthehuman.sans.org/ouch/archives.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Ressurser

Hva er skadevare?:	https://securingthehuman.sans.org/ouch/2016#march2016
Løsepengevirus:	https://securingthehuman.sans.org/ouch/2016#august2016
Sikkerhetskopiering & gjenoppretning:	https://securingthehuman.sans.org/ouch/2015#august2015
Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Sikker bruk av nettskyen:	https://securingthehuman.sans.org/ouch/2016#november2016

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversatt av: NorSIS