OUCH! | Desember 2014

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Hva er antivirus?

Oversikt

Antivirus er et sikkerhetsprogram du installerer på en datamaskin eller en mobil enhet for å beskytte den mot skadevare, ofte bare kalt virus. Skadevare er samlebegrepet for all ondsinnet programvare, som virus, ormer, trojanere og spionprogramvare. Ordet skadevare er en norsk oversettelse av ordet malware, som er bygget opp av ordene malicious og software. Skadevare, er på samme måte, bygget opp av ordene skadelig og programvare. Med mindre det er viktig å markere forskjellen, bruker man ofte bare begrepet virus. Hvis datamaskinen din har blitt infisert av et virus, så kan en angriper fange tastetrykkene dine, stjele dokumenter eller bruke din datamaskin til å angripe andre. Til tross for hva noen tror, så er ikke virus spesifikt til Windows, Mac OS X og Linux kan også bli infisert.

Gjesteredaktør

Jake Williams er grunnlegger av Rendition Infosec (**www.renditioninfosec.com**) og er sertifisert SANS instruktør og kursforfatter. Han er aktiv på Twitter (**@MalwareJake**) og skriver på sin blogg: **malwarejake.blogspot.com**.

Du kan kjøpe antivirus som et eget sikkerhetsverktøy, men det er ofte en del av en sikkerhetspakke. Problemet er at antivirus ikke greier å holde seg oppdatert med angripere og deres metoder, nye virus slippes hele tiden. Det finnes så mange versjoner av virus at det ikke finnes noe antivirusprogram som kan beskytte mot alle sammen. Dette er grunnen til at det er viktig at du forstår at et antivirusprogram vil hjelpe deg med å beskytte datamaskinen, men det kan ikke stoppe alle former for virus. For å forstå dette bedre, la os se på hvordan et antivirusprogram fungerer.

Hvordan antivirus fungerer

Kort fortalt bruker antiviruset to metoder for å identifiserer virus; signaturgjenkjenning og gjenkjenning av oppførsel. Signaturgjenkjenning fungerer på samme måte som det menneskelige immunsystemet. Det skanner datamaskinen for kjennetegn til ondsinnet programvare. Dette fungerer ved at antiviruset har en ordbok med kjente virus, hvis antiviruset finner et program som har kjennetegnet til et kjent virus, så vil antiviruset prøve å nøytralisere programmet. Dette krever at ordboken oppdateres slik at det kan oppdage de nyeste virusene, på samme måte som immunsystemet oppdateres via vaksiner. Antiviruset kan kun beskytte mot det som detekteres som ondsinnet. Problemet er at angripere utvikler nye virus fortere enn antivirusleverandørene greier å utvikle

Hva er antivirus?

signaturer. Dette betyr at: uansett hvor oppdatert antiviruset ditt er, så finnes det alltid et virus som potensielt kan omgå antiviruset og infisere maskinen.

Med gjenkjenning av oppførsel, så prøver ikke antiviruset å gjenkjenne kjente virus, men det overvåker i stedet oppførselen til programmer installert på maskinen. Hvis et program oppfører seg mistenkelig, for eksempel ved at det prøver å aksessere en beskyttet fil eller modifiserer et annet program. Antiviruset vil så detektere denne oppførselen og varsle brukeren. Dette gir beskyttelse mot nye virus som ikke har blitt oppdaget. Problemet er at det genererer for mange falske advarsler. Du, brukeren, blir sannsynligvis usikker på hva du kan tillate og hva du bør blokkere og over tid vil du starte å ignorere advarslene. Etter hvert blir det fristende å trykke "godta" på alle advarslene og maskinen din står helt åpent for angrep. I tillegg, kan man ikke oppdage viruset før det har startet å kjøre på maskinen og du vet ikke hva viruset gjorde før det ble oppdaget, da kan skaden allerede ha skjedd.

Antivirus er en stor del av sikkerheten, men det kan ikke stoppe alle angrep. Du er det beste forsvar, ikke bare teknologi.

Antivirus er en viktig del av beskyttelsen til datamaskiner og mobile enheter. Det er anbefalt å installere og bruke det hvis det er en mulighet. Samtidig er det også viktig å huske at det ikke finnes noe antivirus som kan beskytte deg mot alle former for virus. Til syvende og sist er det deg, og ikke bare teknologi, som er det beste forsvar mot angripere.

Antivirus tips

1. Installer antivirus fra en leverandør du stoler på. Et vanlig angrep er å distribuere falske antivirus, som i realiteten er virus.
2. Sørg for at du har installert siste versjon av antiviruset, eventuelle lisensieringer opprettholdes og at antiviruset er konfigurert til å oppdateres automatisk. Hvis datamaskinen har vært koblet fra Internettet, eller vært avslått i lengre tid, sørg for at du oppdaterer antiviruset med en gang du får tilgang til Internettet igjen.
3. Sørg for at antiviruset automatisk skanner eksterne medier, som USB-minnepinner og sørg for at skanning skjer i sanntid.
4. Følg med på advarsler som kommer fra antiviruset. De fleste advarsler inkluderer en mulighet til å få mer informasjon eller en anbefaling for hva du bør gjøre. Hvis du får en advarsel på en arbeids-PC, sørg for at du kontakter help desk eller overordnet umiddelbart.

Hva er antivirus?

5. Ikke skru av eller avinstaller antiviruset fordi du føler at det gjør PC-en din tregere, blokkerer nettsider eller hindrer det i å installere en applikasjon eller et program. Hvis du skrur av antiviruset vil du utsette deg selv for unødvendig risiko som kan resultere i en seriøs sikkerhetshendelse. Hvis problemet vedvarer på en arbeids-PC, kontakt help desk. Hvis problemet vedvarer på en personlig PC, ta kontakt med antivirusleverandøren, sjekk hjemmesiden eller erstatt antiviruset med et annet antivirus.
6. Ikke installer flere antivirus på samme maskin. Hvis flere antivirus kjører samtidig, vil det sannsynligvis oppstå konflikter og det kan faktisk redusere sikkerheten på datamaskinen.
7. Sørg for at du forstår advarslene som antiviruset gir. Kriminelle kan sette opp veldig realistiske ondsinnete sider som viser realistiske falske antivirusbeskjeder som tilbyr deg å "fikse" datamaskinen. Å klikke på noen av disse knappene kan skade datamaskinen din.

Les Mer

Abonner på månedlig OUCH! nyhetsbrev om sikkerhetsbevissthet, se gjennom OUCH! arkivene og lær mer om SANS sine programmer for sikkerhetsbevissthet hos http://www.securingthehuman.org.

Norsk Versjon

NorSIS er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen. Les mer på www.norsis.no.

Ressurser

Test av antivirus:	http://www.av-test.org/en/
Sosial manipulering:	http://www.securingthehuman.org/ouch/2014#november2014
E-post phishing angrep:	http://www.securingthehuman.org/ouch/2013#february2013
Jeg er blitt hacket, hva nå?:	http://www.securingthehuman.org/ouch/2014#may2014

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis