Det Månatliga Nyhetsbrevet Om Säkerhetsmedvetenhet för Datoranvändare

OUCH!

I DENNA UTGÅVA…

Vad är Anti-Virus?

Översikt

Anti-virus är ett säkerhetsprogram som du installerar på din dator eller mobila enhet för att skydda den från att bli smittade av skadlig kod. Termen “malware” är en catch-all fras för alla typer av skadliga program som virus, maskar, trojaner och spionprogram. I själva verket kommer termen ”malware” från att kombinera orden ”malicious” (sv. skadlig) och ”software” (sv. programvara). Om din dator har blivit infekterad av skadlig kod, kan en cyber angripare fånga alla dina tangenttryckningar, stjäla dina dokument eller använda din dator för att attackera andra. I motsats till vad vissa människor tror, kan alla operativsystem, inklusive Mac OS X och Linux, smittas.

Gäst Redaktör

Jake Williams är grundare av Rendition Infosec (**www.renditioninfosec.com**) och är certifierad SANS instruktör och kurs författare. Han är aktiv på Twitter **@MalwareJake** och skriver på sin blogg på **malwarejake.blogspot.com**.

Du kan köpa antivirusprogram som en fristående lösning, eller så är det ofta inkluderat som en del i ett säkerhetspaket. Problemet är att antivirusprogram inte längre kan hålla jämna steg med cyber angriparna, som ständigt utvecklar och släpper nya typer av skadlig kod. Det finns så många nya versioner av skadlig kod som släpps varje dag att inget anti-virus program kan upptäcka och skydda mot dem alla. Det är därför det är viktigt för dig att förstå att medan antivirusprogram hjälper till att skydda din dator, kan den inte upptäcka eller stoppa alla typer av skadlig kod. För att bättre förstå varför, låt oss titta på hur de flesta av dessa program fungerar.

Hur Anti-Virus Fungerar

I allmänhet finns det två sätt antivirusprogram identifierar malware; signaturdetektering och beteende detektering. Signatur detektering fungerar som det mänskliga immunsystemet. Den skannar din dator efter egenskaper eller kännetecken av kända skadliga program. Den gör detta genom att hänvisa till en ordlista med känd skadlig kod, om något på datorn matchar ett mönster i ordlistan försöker programmet neutralisera det. Liksom människans immunsystem, kräver ordlistan uppdateringar, såsom influensa immunisering, för att skydda mot nya stammar av skadlig kod. Anti-virus kan bara skydda mot vad den känner igen som skadligt. Problemet är cyber angripare utvecklar nya malware så snabbt att antivirusleverantörer inte kan hänga med. Som ett resultat, oavsett hur nyligen antivirus uppdaterades, finns det alltid någon ny variant av skadlig kod som potentiellt kan gå förbi ditt antivirusprogram.

Vad är Anti-Virus?

Med beteendedetektering försöker inte antivirusprogrammet identifiera kända skadliga program, men övervakar beteendet hos programvaror installerade på din dator. När ett program agerar misstänkt, som att försöka komma åt en skyddad fil eller ändra ett annat program, identifierar beteendebaserade antivirusprogram på misstänkt aktivitet och varnar för det. Denna metod ger skydd mot helt nya typer av skadlig kod som ännu inte finns i någon ordbok. Problemet med denna metod är att den kan generera falska varningar. Datoranvändare kan vara osäkra på vad de ska tillåta eller inte tillåta, och med tiden blir okänsliga för alla dessa varningar. Du kanske frestas att klicka på "Acceptera" på varje varning, och lämna datorn öppen för angrepp och smitta. Dessutom när beteendet upptäcks, har den skadliga koden troligen redan körts på din dator och du kanske inte vet vilka åtgärder den tog innan antivirusprogrammet identifierade det.

Även om anti-virus är en viktig del av din säkerhet, kan det inte upptäcka eller stoppa alla attacker. I slutändan är du det bästa försvaret, inte bara teknik.

Anti-virus är en viktig del för att säkra din dator och mobila enheter, när det är möjligt rekommenderar vi att du installerar och aktivt använder det. Dock är den viktigaste punkten att komma ihåg att oavsett hur ditt antivirusprogram fungerar, kan det aldrig skydda dig från alla typer av skadlig kod. I slutändan är du, och inte bara teknik, det bästa försvaret mot dagens cyber angripare.

Anti-virus tips

1. Skaffa antivirusprogram endast från kända, tillförlitliga källor och leverantörer. Det är ett vanligt knep för cyber angripare att distribuera falska antivirusprogram som malware.
2. Kontrollera att du har den senaste versionen av ditt antivirusprogram installerat, att din årliga prenumeration är betald och aktiv, och att ditt antivirusprogram är konfigurerat för att uppdateras automatiskt. Om datorn har varit offline eller avstängd ett tag, kommer ditt antivirusprogram uppdatera sig självt när du slår på den igen eller ansluter den till Internet. Skjut inte upp dessa uppdateringar.
3. Se till att ditt antivirusprogram skannar bärbara medier automatiskt, till exempel USB-minnen, och se till realtidsskydd är på.
4. Var uppmärksam på varningar på skärmen som genereras av din antivirusprogram. De flesta varningar omfattar möjligher att få mer information eller en rekommendation om vad man ska göra härnäst. Om du får en varning på en arbetsdator, se till att kontakta din helpdesk eller din chef omedelbart.

Vad är Anti-Virus?

5. Inaktivera inte eller avinstallera ditt antivirusprogram för att du känner att det gör din dator långsammare, blockerar en webbplats eller hindrar dig från att installera ett program. Om du avaktiverar ditt antivirusprogram utsätter du dig för onödiga risker och det kan resultera i en allvarlig säkerhetsincident. Om problemen kvarstår på en arbetsdator, kontakta helpdesk. Om problemen kvarstår på din dator, kan du prova att kontakta antivirusleverantören, besöka deras hemsida för mer information eller byta ditt antivirusprogram mot en annan produkt.
6. Installera inte flera antivirusprogram på datorn samtidigt. Om du gör det kommer det troligtvis att orsaka att programmen kommer i konflikt med varandra och kan faktiskt minska säkerheten i din dator.
7. Lär dig att känna igen de varningar som ditt antivirusprogram producerar. Cyber angripare kan skapa skadliga webbplatser som har mycket realistiska falska anti-virusvarningar och erbjuder sig att hjälpa dig “fixa” din dator. Genom att klicka på länkarna eller knappar på dessa webbplatser kan du faktiskt skada din dator.

LÄR DIG MER

Prenumerera på det månaltliga OUCH! nyhetsbrevet om säkerhetsmedvetenhet, ha tillgång till OUCH! arkiven, och lär dig mer om SANS lösningar inom säkerhetsmedvetenhet genom att besöka oss på http://www.securingthehuman.org

Swedish Version

OUCH! är översatt av Andreas Bohman och Marcus Andersson. Båda arbetar inom informationssäkerhetsbranchen och har många års erfarenhet i etablering av säkerhetsmedvetenhetsprogramm.

Resurser

Anti-Virus Produktjämförelser:	http://www.av-test.org/en/
Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Nätfiskeattacker:	http://www.securingthehuman.org/ouch/2013#february2013
Jag är Hacked, Vad Gör Jag Nu?:	http://www.securingthehuman.org/ouch/2014#may2014

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Översatt Av: Andreas Bohman och Marcus Andersson

