OUCH!

SANS SECURITY AWARENESS

Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Ja, Du är en Måltavla

Inledning

Många tror att de inte är ett mål för cyberattacker. Att de själva, deras system eller konton inte har ett värde och därför inte behöver skyddas. Detta synsätt kan inte vara längre från sanningen. Om du använder någon form av teknik, oavsett om det är på jobbet eller hemma, tro oss – du är av värde för cyberbrottslingar. Du har tur, du har redan det bästa skyddet som finns mot cyberattacker - dig själv.

Varför du är en måltavla

Det finns många olika typer av brottslingar på Internet idag och de har alla olika motiv. Varför skulle någon vilja attackera dig? Genom att hacka dig kommer de ett steg närmare att nå sitt mål. Nedan följer två vanliga exempel på cyberbrottslingar och varför de riktar in sig på dig.

⚠ **Cyberbrottsling:** Dessa är ute efter att tjäna så mycket pengar som möjligt. Vad som gör Internet så värdefullt för dessa brottslingar är att de enkelt kan attackera alla i världen med bara ett knapptryck och det finns MÅNGA olika sätt de kan tjäna pengar på dig. Till exempel kan de stjäla pengar från din bank, skapa kreditkort i ditt namn och låta dig betala räkningar, använda din dator till att hacka andra personer, hacka dina konton för sociala media eller onlinespel och sälja dessa vidare till andra brottslingar. Listan är nästan oändlig över hur cyberbrottslingar kan tjäna pengar på dig. Det finns hundratusentals brottslingar som vaknar varje morgon med målet att hacka så många som möjligt, inklusive dig, varje dag.

☆ **Riktade attacker:** Denna grupp består av högt utbildade hackers som ofta arbetar för stater, brottssyndikat eller konkurrenter som riktar in sig på din arbetsroll och ditt arbete. Du kanske tror att ditt jobb inte är intressant för hackare men om du visste sanningen skulle du bli väldigt förvånad.

- Informationen du hanterar på jobbet är av otroligt värde för företag och stater.
- Riktade attacker som genomförs mot dig på jobbet behöver inte betyda att de vill hacka dig, men de vill använda dig som en språngbräda för att komma åt någon av dina kollegor eller andra system som du har tillgång till.

- **Dessa attacker kan drabba dig dels på grund av var du jobbar men även vilka företag och organisationer du samarbetar med.**

Jag har Anti-Virus, jag är säker

Även om jag nu är en måltavla så är det inget problem. Jag bara installerar ett anti-virus och brandvägg på min dator så är jag skyddad, eller hur? Tyvärr, det stämmer inte. Många som har installerat säkerhetssystem tror att de är säkra. Tyvärr, det är inte sant. Cyberbrottslingar fortsätter att utvecklas och blir bättre. Många av deras attackmetoder kan enkelt kringgå olika säkerhetssystem. Till exempel kan de ofta skapa ett unikt virus som ditt antivirus inte klarar av att detektera. De kan kringgå ditt e-postfilter med en riktad phising-attack eller ringa till din telefon för att försöka lura till sig information om kreditkort, lösenord eller annan information som nyttjas till bedrägerier. Teknik och säkerhetssystem spelar en viktig roll i att skydda dig men du är alltid det sista och bästa försvaret.

Lyckligtvis är det inte speciellt svårt att vara säker, här är sunt förnuft det bästa försvaret samt att tillämpa några enkla metoder. Om du får ett e-postmeddelande eller telefonsamtal som är extremt brådskande, underligt eller misstänksamt är sannolikheten hög att det handlar om en cyberattack. För att säkerställa att dina datorer och enheter är säkra, håll dom uppdaterade med automatiska uppdateringar. Slutligen, använd alltid unika och starka lösenord för dina olika konton. Om något låter för bra för att vara sant är det oftast det. Att vara cybermedveten är i slutändan det bästa försvaret. Är du inte säker på var du ska börja? Överväg att prenumerera på det månatliga nyhetsbrevet OUCH! från sans.org/ouch.

Gästskribent

Matt Bromiley *(@mbromileyDFIR) är expert inom Incident Response och Digital Forensic med över 8 års erfarenhet. Han har arbetat med organisationer och hanterat incidenter över hela världen. Matt är även instruktör inom Incident Repsonse och Digital Forensic för kurserna SANS FOR508 och FOR572.*

Källor

Stop That Malware: https://www.sans.org/u/L1J
Social Engineering: https://www.sans.org/u/L1O
Phone Call Scams: https://www.sans.org/u/L1T
Passphrases: https://www.sans.org/u/L1Y
Poster - You Are a Target: https://www.sans.org/u/L23

OUCH! Publiceras av SANS Security Awareness och distribueras under Creative Commons BY-NC-ND 4.0-licens. Du kan fritt distribuera nyhetsbrevet eller använda det i ditt medvetenhetsprogram så länge du inte ändrar innehållet i nyhetsbrevet. För översättning eller mer information, vänligen kontakta www.sans.org/security-awareness/ouch-newsletter. Redaktion: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Översatt av: Erik Täfvander & Johan Ahlberg