Verksamheten för samhällets informations- och cybersäkerhet
CERT-SE
08-678 57 99
cert@cert.se

Snabbrapport

Aktuellt problemområde: Phishing

Phishing är idag en vanligt förekommande metod som används i syfte att lura användare på känslig information (e.g. lösenord och bankuppgifter) eller leverera skadlig kod. Phishing förekommer i flera former, där epost som uppmanar mottagaren att klicka på en länk, öppna ett dokument eller fylla i personliga uppgifter hör till de vanligaste. Under de senaste åren har det skett en övergång från massiva utskick riktade till så många mottagare som möjligt till den mer inriktade formen benämnd *spear phishing*. Även om virusskydd och spamfilter är bra skyddsåtgärder så är det mottagaren som har störst möjlighet att identifiera och avvärja en phishingattack.

Bakgrund

Det finns idag flera olika varianter av phishing. Vissa syftar till att leverera skadlig kod, andra ämnar att lura av användare känslig information. Syftet kan skilja sig mycket mellan olika varianter men när det kommer till levereransmetoder finns det i stort sett två varianter:

Den första består av massiva utskickskampanjer där man vill nå så många mottagare som möjligt, oavsett vilka de är. Dessa e-postmeddelanden kännetecknas av att de är maskinellt översatta vilket resulterar i ett antal tydliga indikatorer på att något inte står rätt till. Stavfel, felaktig grammatik, avsaknad av punkter och versaler samt att epostadressen kan skilja sig kraftigt från den organisation angriparen utger sig att vara ifrån är exempel på sådana indikatorer. Anledningen till de tydliga signalerna kan bero på olika faktorer. I en del fall är felaktigheterna medvetna i syfte att sålla ut de mest sårbara mottagarna. Därefter kan angriparna fokusera sina resurser på de mottagare där möjligheterna att lyckas med sitt bedrägeri är allra störst. I andra fall bryr de sig inte om vilka de skickar till utan fokuserar endast på att få ut maximalt antal meddelanden, vilka sedan sprider sig över nationella gränser och språkområden och därmed resulterar i de konstiga formuleringarna.

Den andra varianten, kallad *spear phishing*, blir mer vanlig idag [1]. *Spear phishing* är betydligt svårare att upptäcka då angriparna lagt större energi på att skriva riktade personliga meddelanden till specifikt utpekade mål. De kan till exempel innehålla namn på personer som faktiskt finns i organisationen och därmed

uppfattas som autentiska och legitima [2]. Allt i syfte att minimera risken för att mottagaren skall upptäcka bluffen. Eftersom meddelandena är riktade sker inte spear phishing via massutskick.

Angreppsmetoder

Den vanligaste angreppsmetoden för phishingattacker är via e-post. Den ökade användningen av sociala medier har lett till både en ökad tillgång till personlig information om potentiella mål samt till en ny angreppsmetod i form av chattmeddelanden. Andra kanaler som förekommer är telefonsamtal, SMS och fejkade hemsidor. Det är även vanligt att angriparen försöker pressa fram en snabb respons genom att sätta mottagaren under stress. Hot om att stoppa åtkomsten till ett konto eller antyda att kontot blivit hackat och att säkerhetsåtgärder måste utföras snarast är exempel på detta.

Mänskliga skyddsåtgärder

En av de mest effektiva skyddsåtgärderna är utbildning av personalen så att de på egen hand kan identifiera potentiella phishingattacker. Nedan finns ett antal saker att tänka på i syfte att skydda sig mot phishingattacker:

- **Undersök den faktiska avsändaradressen** - I moderna mailklienter göms oftast avsändaradressen bakom ett namn. Då namn inte måste vara unika är detta ett effektivt sätt att gömma den suspekta avsändaradressen.
- **Verifiera avsändare** – Innan bifogade dokument eller filer öppnas bör avsändarens identitet verifieras. Är det så att en ny kollega har börjat eller har en angripare kommit in? Har en tjänsteleverantör byt e-postadress? Ifall avsändaren inte kan verifieras bör undersöka meddelandet extra noggrant efter indikationer på phishingförsök.
- **Analysera språket** – Innehåller texten grammatiska fel, stavfel eller verkar det som att texten blivit översatt av ett verktyg är detta en tydlig indikation att e-postmeddelandet är phishing.
- **Undersök länkarna** – Det är alltid en bra idé att undersöka länkarna noga. Är det en länk till en hemsida man ofta besöker kan man jämföra länken efter skillnader. Förkortade länkar (e.g. TinyUrl) är ett sätt att dölja den faktiska adressen av länken.
- **Skriv själv** - Använd inte länkar som finns i mailen. Vid uppmaningar att gå in på en specifik hemsida, surfa in på den själv och använd inte länken.

Tekniska skyddsåtgärder

En del phishingattacker försöker extrahera information från mottagaren genom att installera skadlig kod på mottagarens dator. Genom att hålla virusskydd uppdaterade ökar chansen att skadlig kod blir upptäckt och oskadliggjord. Mail Gateways som kontrollerar inkommande mail mot kända phishing avsändare (e.g.

IP-adresser av mailrelän) kan stoppa phishingförsök innan de ens når fram till en eventuell mottagare. Då majoriteten av phishingattackerna sker via e-post är restriktiva inställningar på e-postklienter ett bra skydd. Genom att blockera att bifogade dokument öppnas automatiskt ger mottagare möjlighet att undersöka meddelandet ifall de kan innebära en potentiell phishingattack. Andra effektiva åtgärder är att inte tillåta att fjärrinnehåll laddas in automatisk eller att script får köras utan mottagarens godkännande. Det är inte heller alltid som phishingattacker upptäcks, därmed är det god praxis att sätta utgångsdatum på lösenord så att de med jämna mellanrum måste bytas ut.

Sammanfattningsvis, phishing är en angreppsmetod som angripare använder i syfte att med minimalt arbete lura av personer på känslig information. Genom att använda unika lösenord på olika hemsidor och till olika tjänster minskar risken att en lyckad phishingattack leder till att en angripare kan angripa samma användare på flera siter. Man ska vara medveten om att en phishingattack inte har lyckats förrän mottagaren delger sig utav informationen eller klickar på någon länk. Tar man sin tid och undersöker mailet noga har man stor chans att upptäcka attacken.

Rapportera phishingangrepp till CERT-SE

Upptäckta och även misstänkta phishing angrepp kan rapporteras in till CERT-SE via mejladressen phishing@cert.se. Inskickade phishing angrepp hjälper CERT-SE bygga upp en uppfattning av vilka phishingkampanjer pågår i Sverige, samt varna för kända avsändare eller rubriker som förekommer i nya phishingkampanjer.

Mer information

https://blog.kaspersky.com/how-to-avoid-phishing/6145/

https://digitalguardian.com/blog/phishingattack-prevention-how-identify-avoid-phishingscams

Referenser

[1] www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf

[2] Protecting against spear-phishing Bimal Parmar, 2012, Elsevier