E-mail-snyd rettet mod virksomheder bliver sværere og sværere at gennemskue

Velkommen tilbage til sikkerhedssiderne i Alt om DATA. Denne gang kigger vi på fænomenet spear phishing samt afarten af det samme, som kaldes for CEO fraud. Begge dele er blevet et stigende problem i mange virksomheder, og de kan være svære eller næsten umulige at gardere sig mod.

Målrettet phishing

Lad os starte med at definere hvad phishing er for noget. Vi ved alle, hvad spam er, nemlig de e-mails, vi alle sammen modtager, der f.eks. foregiver at kunne sælge os produkter, der kan forøge vores "ydeevne" til en billig penge. Disse e-mails bliver sendt til millioner af modtagere hver dag. Spear phishing er derimod e-mails, der er mere målrettede.

En spear phishing e-mail er typisk rettet imod bestemte personer i en virksomhed. Målet er at få modtageren til at klikke på et link i e-mailen eller åbne en vedhæftet fil. Når brugeren klikker på linket eller åbner filen, vil personens computer blive inficeret med en virus, hvis formål er at give angriberen kontrol, så han/hun kan udvide sine beføjelser i netværket. Endemålet vil være at få en adgang, der svarer til Domain Administrator på et Windows-netværk eller root på et Linux/Unix-netværk.

Mange af de mest omtalte indbrud i virksomheder er startet med, at en bruger i virksomheden har modtaget en spear phishing e-mail og har klikket på noget, som de ikke skulle have klikket på. Sony, RSA og HBGary Federal er alle sammen virksomheder, der er blevet kompromitteret af en spear phishing e-mail.

De to virksomheder RSA og HBGary er endda i sikkerhedsbranchen, hvilket viser, at selv dem, der arbejder med at beskytte os imod hackerangreb, er sårbare overfor de samme typer af angreb, som vi døjer med. Hvad angår RSA, så fik angriberne adgang til kronjuvelerne, der er RSA's token-løsning. HBGary Federal eksisterer ikke mere. Alt afhængig af hvad angriberne får adgang til, så kan det have store konsekvenser for offeret at blive udsat for sådan et angreb eller et angreb i det hele taget.

E-mails virker legitime

Men hvorfor virker disse spear phishing e-mails? Vi har efterhånden i mange år vænnet os til at genkende de almindelige spam-mails, men en af forskellene mellem disse og en spear phishing e-mail er, at der bliver lagt mere vægt på udformningen af en spear phishing e-mail, end der gør på en spam-mail. F.eks. vil den hjemmeside, som et link i en spear phishing e-mail peger på, se legitim ud. Der vil være medtaget alle de logoer og den navigation, som brugeren er vant til fra den virkelige hjemmeside. Selve e-mailen vil også se professionel og virkelig ud. Teksten i e-mailen vil tillige referere til ting og sager, som modtageren vil genkende fra sin dagligdag. Kort sagt, så vil der ikke umiddelbart være nogen grund til at mistænke, at e-mailen er falsk, og det er grunden til, at disse spear phishing e-mails virker.

Man skulle tro, at diverse antivirus-programmer og IDS/IPS burde fange, at der er tale om noget mistænkeligt, når brugeren åbner en vedhæftet fil eller får noget installeret fra en hjemmeside. Her kommer vi til det virkeligt slemme ved spear phishing. Dem, der anvender denne type af angreb, er fast besluttede på at trænge ind på virksomhedens netværk, og de er villige til at bruge den tid og de ressourcer, der skal til for at komme ind.

Bruger 0-day sårbarheder

0-day sårbarheder er et hul i software, som leverandøren af softwaren ikke er klar over eksisterer, og som ikke er blevet brugt til et angreb før. Når en sårbarhed ikke er blevet brugt før, så ved antivirusleverandøren ikke noget om den. Heller ikke leverandøren af IDS/IPS vil have nogen mulighed for at beskytte imod angrebet. Antallet af de 0-day sårbarheder, der bliver fundet om året, stiger nærmest eksponentielt. I Alt om DATA har vi beskrevet, hvordan der foregår handler med disse typer af huller i software. Hvis du har brug for at genlæse artiklen, kan du finde den i Alt om DATA nr. 5.

Værn mod spear phishing

Alle de forskellige leverandører af hardware og software til beskyttelse af vores netværk kæmper en ulige kamp imod den stadigt stigende mængde af angreb, der hele tiden forekommer. De forsøger konstant at udvikle deres produkter til at kunne opdage nye sårbarheder og typer af angreb, men som det ser ud nu, er det en ulige kamp. Måske vil Big Data eller den forskning, der sker i kunstig intelligens kunne hjælpe i fremtiden, men det er kun tiden, der vil kunne vise, om det bliver en løsning.

Lige nu er der kun én vej frem, og det er træning, træning og atter træning af slutbrugerne. Hvis brugerne hele tiden er opmærksomme på, at de kan modtage en spear phinshing e-mail, hvornår det skal være, så vil de være en del af løsningen i stedet for en del af problemet. Hvis virksomhederne gør brugerne til en integreret del af virksomhedens sikkerhedssetup, så vil virksomheden være langt mere sikker imod denne type af angreb, og brugerne vil føle, at de er en del af løsningen, i stedet for at blive revset af sikkerhedsafdelingen.

CEO fraud

Som nævnt i begyndelsen er CEO fraud et relativt nyt fænomen, der er blevet føjet til værktøjskassen for hackere, der fokuserer på økonomisk gevinst i deres angreb på virksomheder. I 2015 kom FBI frem med en advarsel, der sagde, at antallet af CEO fraud-angreb var steget med 270 % i 2014. De summer, der var blevet mistet til denne type af snyd, var på det tidspunkt 2,3 milliarder dollars, og der var virksomheder i 79 lande, der var ofre for angreb af denne type.

Også Danmark er blevet angrebet på denne måde. For nylig kom dansk politi frem med oplysninger om, at to danske virksomheder tilsammen havde mistet 140 millioner kroner til CEO fraud, men mon ikke det reelle tal er meget højere. Det er nemlig ikke alle virksomheder, der er villige til at gå til politiet med oplysninger om, at de er blevet snydt for millioner af kroner.

Som nævnt, så består angrebet typisk i, at en medarbejder modtager en mail, der ser ud til at komme fra chefen for det hele. Der skal lynhurtigt overføres nogle penge til en konto i udlandet, der skal bruges til et virksomhedsopkøb. Mailen kan også se ud som om, den kommer fra virksomhedens advokatkontor, men uanset hvor den kommer fra, så vil det se ud som om, den er blevet sendt fra virksomhedens netværk og kommer fra chefens e-mail. Hele kommunikationen vil emme af at være tidskritisk, og det hele skal foregå på den halve tid for ikke at give nogle af dem, der er involveret, tid til at stoppe op og tænke over, hvad det er der foregår.

Igen her, er det kun træning af brugerne, der kan beskytte virksomheden imod den slags snyd. En anden ting, der kan hjælpe, er at indføre en regel om, at der skal to personer til at godkende overførsler til udlandet af beløb over en vis størrelse. På den måde vil der være mere end én person, der kan stoppe op og tænke et øjeblik over, hvad det er, der foregår. Budskabet her er, at slutbrugerne skal involveres i sikkerhedsberedskabet i virksomheden. Hvis virksomheden fortæller de ansatte, når der har været en hændelse, uden at nævne navne, så er de hele tiden opmærksomme på, at brud på it-sikkerheden er en reel trussel. ■