Ny sikkerhedstrussel: Phishing på sms og sociale medier!

Hos Systemcenter Randers har vi længe haft stor fokus på ransomware, malware og phishing i e-mails. Vi har tidligere lavet en længere annonce der beskrev fænomenet og gav virksomheder otte effektive råd, til at forebygge og forhindre uvedkommende overtager dine værdifulde it-data. Den nyeste trend blandt hackere er tilsyneladende klar, og med stor succes, nemlig phishing på sms og sociale medier.

”Phishing er et fænomen, hvor hackere og svindlere forsøger at franarre godtroende internetbrugere deres værdifulde it-data.”

Den stigende fokus på phishing i e-mails, gør at de fleste medarbejdere i virksomheder, tænker en ekstra gang, før de trykker på et link i deres indbakke. Men med større fokus og større forsigtighed, forsøger hackere at finde andre veje ind til dine følsomme it-informationer. Det nyeste sikkerhedshul er smishing. Som navnet antyder, har det noget med phishing at gøre – dog på SMS. Phishing på SMS, smishing, er et fænomen der er på vej til at vinde indpas hos hackerne. Med god grund. Vi er nemlig, åbenbart, ikke særligt opmærksomme på, hvad vi trykker på i en SMS.

En ny undersøgelse udført af Alexandra Instituttet, i samarbejde med DBI, undersøger instituttet, hvor mange brugere de kan få til at trykke på et phishing link i sms. For at det skulle være yderst relevant, målrettede de angrebet mod virksomheder med kritisk infrastruktur. Et forsvarsinstitut, en virksomhed i olieindustrien, og et generelt sikkerhedsfirma. Virksomheder der alle burde være klar over den tidsaktuelle trussel fra hackere og malware/ransomware.

89 % blev ramt af phishing på sms

Forsøgets resultat endte med, at hele 89 % af brugerne i virksomhederne, endte med at trykke på phishing-linket i sms’en. For at holde resultatet op mod almindelig phishing, blev der også sendt en e-mail med link til samme virksomheder. Her blev der trykket på linket hele 40 % af gangene, hvilket også er et meget højt antal, hvis vi holder resultatet op imod den skade et enkelt angreb kan foretage.

Ikke desto mindre, kan vi ud fra resultaterne konkludere, at hackerne med god grund, forsøger at flytte deres angreb over på sms. Succesraten er større og der er mulighed for både, at ramme medarbejderne på sms og e-mail på samme tid.

Phishing på sociale medier

For ikke at ramme brugerne personligt, blev undersøgelsen ikke udført på de sociale medier. Det estimeres dog, at der er den samme sikkerhedstrussel på de sociale medier, som der er på sms. Sociale medier bliver en større og større del af virksomheders brand og markedsføring. Samtidigt med at mange medarbejdere tjekker deres profiler i arbejdstiden. Derfor er der chance for, at hvis en medarbejder bliver ramt af phishing på sociale medier, er det mens medarbejderen sidder på virksomhedens netværk.

Undervis dine medarbejdere i viden om phishing

Vi har sagt det før, og vi siger det gerne igen. Der skal oftest ikke mere til, før at virksomhedens it-infrastruktur bliver lagt ned, end en enkelt medarbejder der trykker på et forkert link. Derfor er det vigtigt at alle medarbejdere i virksomheden, kender til truslen og ved hvordan de skal forholde sig links i e-mails og nu også på sms.