OfficeGrip

Bescherm je

ZWAKSTE BEVEILIGINGSSCHAKEL:

eindgebruikers

EEN GIDS VOOR DE VERDEDIGING TEGEN SOCIAL ENGINEERING-AANVALLEN

OfficeGrip

AMATEURS HACKEN SYSTEMEN. PROFESSIONALS HACKEN PERSONEN.

— Bruce Schneier, CTO
Counterpane Internet Security, Inc.[1]

2015 WAS EEN BELANGRIJK JAAR in de wereld van de netwerkbeveiliging. Voor de eerste keer waren er meer social engineering-aanvallen dan aanvallen op kwetsbaarheden in software. Dit is een serieus probleem.

Als organisaties productief willen blijven, moeten hun medewerkers overal kunnen werken, op elk apparaat en vaak samenwerken met mensen op de hele wereld. Deze mobiliteit stuurt niet alleen de behoefte aan het veilig delen van bestanden en e-mailaccounts, maar ook een fundamentele verschuiving in onze aanpak van computerbeveiliging.

Sinds januari 2015 is het aantal slachtoffers dat door de FBI is geïdentificeerd, vergroot met 270% en kost het het bedrijfsleven meer dan $ 2,3 miljard.[2] De boodschap voor netwerkbeveiligings professionals is duidelijk. Hackers hebben het voorzien op de zwakste schakel in elke veiligheidszone: de eindgebruiker.

Dit boek is een gids om je te helpen social engineering-aanvallen te detecteren en te voorkomen en om beter te begrijpen hoe je je organisatie kunt verdedigen tegen wat intussen de belangrijkste globale cyberbedreiging is geworden.

Wat is SOCIAL ENGINEERING?

Social engineering vindt plaats wanneer iemand manipulatie, invloed of misleiding gebruikt om een ander persoon zover te krijgen informatie vrij te geven of bepaalde acties uit te voeren ten gunste van een hacker.

Hackers maken vaak misbruik van echte beveiligingsgaten in je netwerk. Bij bedrijven van elke grootte, kunnen lagen geavanceerde computerbeveiliging ineen paar seconden worden ontweken, omdat één medewerker (vanwege vertrouwen, gebrek aan bewustheid of roekeloosheid) bedrijfsgegevens prijsgeeft aan iemand met kwade opzet.

Je medewerkers kunnen tot alles verleid worden, van het toestaan dat iemand met ze door de toegangssluis van een datacenter loopt tot het delen van hun wachtwoorden of gebruikers-id's via de telefoon. Social engineers gaan heel ver om toegang te krijgen tot gegevens die ze kunnen exploiteren, zoals:

- **PERSOONLIJKE GEGEVENS** wachtwoorden, accountnummers
- **BEDRIJFSGEGEVENS** telefoonlijsten, ID-badges
- **SERVERGEGEVENS** servers, netwerken, niet-openbare URL's

Je eerste verdediging is dan ook vertrouwd raken met social engineering-technieken.

Dus,hoe klinkt een social engineer?

Je zou denken dat social engineers makkelijk te herkennen zijn, maar heel vaak klinken ze net als de mensen waar je iedere dag op het werk mee in aanraking komt.

AAN DE TELEFOON

"Dit is Kevin van IT. We hebben een melding gekregen dat er zich een virus bevindt op de computers van jouw afdeling."

Eén van de meest voorkomende trucs: een hacker doet zich voor als een helpdeskmedewerker van de IT-afdeling om gevoelige gegevens zoals wachtwoorden van een nietsvermoedende medewerker te verzamelen.

BIJ DE ONTVANGSTBALIE

"Hoi, ik ben de onderhoudsmedewerker van HP en ik geloof dat Ellen me om 13:00 uur verwacht."

Dat is waarom het zo belangrijk is dat goedbedoelende werknemers en andere bekenden onderwezen worden hoe en waarom ze het doelwit kunnen zijn en wat ze moeten doen als ze een potentiële bedreiging vermoeden.

BIJ DE TOEGANG TOT KANTOOR

"Oh. Wacht, kun je de deur even vasthouden? Ik heb mijn sleutel-/toegangspas in de auto laten liggen."

Mensen willen graag helpen en onderschatten vaak de risico's van het helpen van onbekenden en dat kan een riskante combinatie zijn.