

Aanvallen van binnenuit

Bedrijven (over)beveiligen hun gateways tegen inkomende verbindingen. Vaak vergeten ze echter hun netwerk te beveiligen tegen allerlei mogelijke interne aanvallen. In deze editie van CBM behandelen Righard Zwienenberg en Eddy Willems Social engineering en de gevaren van sociale netwerken.

TEKST: RIGHARD ZWIENENBERG
EN EDDY WILLEMS

Veel externe verbindingen hebben toegang tot het interne netwerk, zoals bijvoorbeeld leveranciers, telewerkers en VPN-verbindingen. Zelfs wanneer u denkt dat u alles beveiligd heeft, kunt u toch nog het slachtoffer worden



De Belg **Eddy Willems** is Security Evangelist bij G Data Software AG. Hij is al sinds 1989 actief op het gebied van IT-beveiliging. Tijdens die periode heeft hij gewerkt voor invloedrijke organisaties, zoals EICAR, waarvan hij medeoprichter en directeur pers en informatie is, verschillende CERT-instellingen, internationale politiediensten, de organisatie achter de WildList en commerciële ondernemingen zoals NOXS en Kaspersky Lab Benelux. Als Security Evangelist bij G Data vormt hij de link tussen de technische complexiteit van IT-beveiliging en de gebruiker.

van aanvallen van binnenuit. Deze en volgende maand wordt een overzicht gegeven van veel mogelijke scenario's van interne aanvallen.

Social engineering en privacy

Social engineering-aanvallen op de beveiligingssystemen maken gebruik van een combinatie van intermenselijke vaardigheden, onderzoek en technische knowhow. Er wordt geprofiteerd van de menselijke natuur om zo de privacy van bedrijven en individuen te kunnen schenden.

Social engineering heeft meer te maken met de manipulatie van mensen dan technologie om de beveiliging van een bedrijf te doorbreken. Het blijft het grootste beveiligingsrisico, ondanks onze vooruitgang op technologisch vlak. Veel van de meest schadelijke aanvallen zijn het gevolg van social engineering, niet van elektronisch hacken of inbreken.

Social engineering is gebaseerd op inzicht in het menselijke gedrag en het vermogen om anderen te overtuigen informatie vrij te geven. Het overtuigen is een kunst op zich. Sommige personen hebben een natuurlijke gave om te manipuleren, terwijl anderen de vaardigheid ontwikkelen door oefening met positieve en negatieve resultaten.

Probing

Alles dat informatie opslaat of toegang heeft tot informatie kan het slachtoffer worden van een social engineering-aanval en niemand binnen het bedrijf is veilig. Hoewel een oude factuur of telefoonlijst op zich niet gevaarlijk lijkt, kan de aanvaller op basis van deze informatie een relatie ontwikkelen door 'interne' kennis te gebruiken om op

korte termijn vertrouwen te winnen. Elektronische systemen worden het slachtoffer van rechtstreekse aanvallen of probing. Door een systeemnaam of IP-adres te leren, kan een aanvaller zich voordoen als een netwerktechnicus. Er is waarschijnlijk een grote hoeveelheid informatie over uw bedrijf of personeel beschikbaar op het internet in openbare- of privé databases. Aanvallen die gebruik maken van social engineering krijgen vaak toegang tot bedrijfssystemen, al is het maar door over iemands schouder mee te kijken tijdens een bezoek aan het bedrijf.

Alle informatie, hoe klein ook, is waardevol voor een aanvaller. Het is belangrijk te weten dat social engineering-aanvallen cyclisch gebeuren. Aanvallers

