OUTFLANK

Samenvatting presentatie "De hacker vertelt…"

Gedurende de presentatie hebben we het aanvalspad van een hacker of cybercrimineel doorlopen aan de hand van drie vragen. Hieronder herhaal ik deze vragen en geef ik de belangrijkste tips per stap.

Hoe komt de hacker aan mijn gegevens?

Ik heb de deelnemers meegenomen in de wereld van datalekken. Regelmatig worden websites gekraakt en soms besluit de hacker om de gecompromitteerde gegevens op het internet te publiceren. Dit is de afgelopen jaren bijvoorbeeld gebeurd bij LinkedIn, DropBox en Adobe. Dit resulteert erin dat van heel mensen hun wachtwoord al een keer is gelekt. Je beperkt het gevaar van datalekken met de volgende tips:

- Check of je zelf al voorkomt in één van de bekende datalekken. Dit kan bijvoorbeeld op http://www.haveibeenpwned.com of http://www.scatteredsecrets.com.
- Wachtwoord hergebruik voorkomen. Als je overal verschillende wachtwoorden gebruikt, dan is de impact van een datalek op jou een stuk kleiner. Een voorbeeld van een gratis wachtwoordenkluis is KeePass.
- Gebruik van tweestapsverificatie. Heldere uitleg hierover vind je op: https://veiliginternetten.nl/themes/situatie/wat-tweestapsverificatie/

Hoe komt de hacker in mijn systeem?

Aan de hand van een demonstratie heb ik het gevaar van de drive-by-download getoond: de methode waarbij een hacker jouw systeem binnendringt als je niet de laatste beveiligingsupdates hebt geïnstalleerd. Hoe bescherm je je hiertegen?

- Zorg ervoor dat je altijd de laatste beveiligingsupdates hebt geïnstalleerd. Configureer waar updates op "automatisch installeren" voor alle software.

Wat wil de hacker met mijn systeem?

In heel veel aanvallen maken cybercriminelen gebruik van malware: ze installeren malafide software nadat ze toegang hebben gekregen tot je systeem. Dit soort malware wordt vervolgens gebruikt voor aanvallen op internetbankieren op jouw PC, het versleutelen van je bestanden (ransomware) of het onderscheppen van toetsaanslagen voor het stelen van creditcardgegevens. Belangrijk is om jezelf goed te beschermen tegen malware met de volgende tips:

- Installeer een goed beschermingspakket. Suggesties vind je op: https://www.pcmag.com/article2/0,2817,2369749,00.asp.
- Zorg ervoor dat je goede backups hebt en dat deze op een veilige plek worden opgeslagen. Zo beperk je de schade in het geval van een incident met ransomware.

Voor nog veel meer goede tips: check www.veiliginternetten.nl en www.laatjeniethackmaken.nl.

Tot slot is het belangrijk om niet paranoïde te worden. Geniet van al het moois dat digitalisering en internet je brengt. Met deze simpele basistips en een dosis gezond verstand, kun je veilig digitaal werken.

Stan Hegt
+31 6 1188 5039
stan@outflank.nl
www.outflank.nl/stan