Enschede 7 november 2019 – Risk & Resilience festival

Hebt u ook weleens opgekeken tegen een taak die u, omdat u die nog nooit eerder had gedaan, erg moeilijk leek maar eenmaal begonnen en afgerond dacht van, Heb ik hier zo tegenop gekeken? Omdat we er nog geen kennis van hebben en dat we het nog nooit hebben gedaan wil niet zeggen dat het moeilijk is. Ongeveer dit gevoel hield ik over na de presentatie over Information Security 101.

Het onderwerp van de presentatie was “Hoe zou jij je eigen bedrijf aanvallen?” Dit seminar werd in het Endels gegeven door Raffaele Mazzitelli, een medewerker van het bedrijf Xebia.

Raffaele opende met een leuke anekdote over hoe hij op een ochtend bij het bedrijf waarvoor hij werkte binnenkwam en daar door een collega werd opgewacht. Zij was namelijk de sleutel kwijt van haar kast met daarin de creditcard van de zaak die zij toch echt die ochtend nodig had om zaken mee te betalen. Raffaele, een (informatie)beveiligingsexpert, had namelijk ook kennis van lockpicking en dat was precies de vaardigheid die zij op dat moment nodig had. Uiteraard reisde Raffaele niet dagelijks met zijn lock-picksetje op zak maar hij wilde toch wel even kijken of hij iets kon betekenen voor de collega in nood.

De kast in kwestie bleek een bureauladeblok die Raffaele door het duwen op 2 plekken vakkundig zonder sleutel - en zonder de kast te vernielen - geopend kon worden.
Beiden waren verbaasd. De collega die de creditcard nodig had dat het zo makkelijk en snel ging, Raffaele omdat de collega blijkbaar in de veronderstelling was dat het bureauladeblok een veilige opberglocatie zou zijn voor de bedrijfscreditcard. Na deze korte maar leuke anekdote begon de eigenlijke presentatie.

Raffaele behandelde een aantal onjuiste aannames die bij veel mensen spelen.

1. Macs kunnen geen virussen krijgen dus een virusscanner is niet nodig.
   Hoewel er wel veel minder virussen zijn voor Mac, zijn ze er wel.
2. Ik zie niets gebeuren op het beeldscherm dus er is niets gebeurd.
   Veel virussen draaien op de achtergrond van de pc zonder dat je als gebruiker daar iets van merkt. Ook worden bestaande databases en wachtwoorden gebruikt om je te hacken.
3. Er is veel computerkracht nodig om een bedrijf te hacken.
   Er zijn veel systemen op het internet al gehackt. Deze systemen (bots) kun je kopen en gebruiken voor een grote aanval. Een andere methode is om een computer in het netwerk aan te vallen en dan van daaruit van binnenuit de bedrijfsservers aan te vallen.
4. Als er een goed slot op de deur zit kom je niet binnen.
   Dat klopt maar dan moet je hem wel op slot doen.
5. Slotenkraken is heel moeilijk.
   Raffaele liet een aantal leuke filmpjes zien over hoe cilindersloten werken en hoe je die dus zonder al te veel inspanning kunt openen/kraken.
6. Ik heb het niet op die manier geconfigureerd dus dat zou niet moeten kunnen.
   Veel softwaretoepassingen worden niet veilig geleverd. Installeer dus altijd de laatste updates om te voorkomen dat ze iets gaan doen waarvoor ze niet bedoeld zijn.
7. Hacken is moeilijk.
   Aan de hand van een aantal zoekmachines en databases werd ons getoond hoe je heel snel de juiste informatie kan vinden over een bepaald onderwerp.

Belangrijkste take-aways van deze presentatie:

1. Hacken/inbreken is niet zo moeilijk als je denkt. Zoek eens op het onderwerp en u zult merken dat er heel veel how-to’s en filmpjes over bijna elk beveiligingsonderwerp te vinden zijn.
2. Vertrouw niet zomaar op je beveiliging, selecteer goede producten en gebruik ze op de juiste manier. Oftewel deuren op slot.

Gerton
Student Risicomanagement aan de Universiteit Twente