Hackers

Frank Brokken
f.b.brokken@rug.nl

ICT-security

Frank Brokken is security manager bij het RC. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.

En dan vraag je je als 'security manager' toch af wat er mis is gegaan, wanneer je plotseling wordt geconfronteerd met het bericht dat er meer dan 200 computers van de RUG zijn 'gehacked' ....

Tja...

De universiteit is geen bank...

Vrije kennisuitwisseling

De RUG-netwerkorganisatie is nou eenmaal niet zo opgezet als een bank. Nee, tot verbazing van bedrijven die ons, ongetwijfeld met de beste bedoelingen, hun hulp aanbieden bij het voorkomen van herhalingen: we hebben geen globale firewall, we controleren niet welke informatie op het internet door de RUG-medewerkers en -studenten wordt bezocht, en veel RUGnet-gebruikers kunnen naar eigen inzicht installeren wat ze maar willen op de computers die door de RUG ter beschikking worden gesteld.

Nee, we zijn een universiteit en voor een universiteit is vrije uitwisseling van kennis essentieel; beknotting van de mogelijkheden die door het internet wordt geboden, betekent een ontoelaatbare aantasting van de vrije uitoefening van de wetenschap.

Tja...

Als security manager vraag je je dan toch ook wel eens af of je nou echt in de woestijn staat te roepen. Laat me een veel gehoord bezwaar tegen beveiliging herhalen: beveiliging zou de mogelijkheden om nu eens echt aan het werk te gaan te zeer beknotten. Zou dat zo zijn? Als u in een auto stapt, is het aangespen van een veiligheidsriem dan zo'n beknotting? Als u een auto heeft, is het laten uitvoeren van een jaarlijkse APK-keuring of onderhoudsbeurt dan zo'n aantasting van uw mogelijkheden om gebruik te maken van uw auto? Kom nou...

Hackersprijs

Nee, dat beveiliging alleen maar tot beperkingen zou leiden is allemaal flauwekul. Smoesjes om je aan je eigen verantwoordelijkheid te kunnen onttrekken.

Laten we even terugkomen op de hack van meer dan 200 RUG-computers. Hoe vervelend ook, maar een van de wapenfeiten van onze 'tegenpartij' was dat ze toegang hadden gekregen tot de installatieserver van de Universitaire werkplek (UWP), waardoor wij een deel van hun werk voor hen hebben uitgevoerd. Elke keer dat er een nieuwe UWP werd geïnstalleerd, zorgden we er zelf voor dat de nieuwe werkplek direct toegankelijk was voor de hackers. Zoiets verdient een prijs in de hackerwereld, lijkt me. Vervelend voor ons, en je vraagt je onwillekeurig af hoe het zover heeft kunnen komen.

Zou er geen integriteitscontrole op de UWP-software worden uitgevoerd? De software die op de installatieservers staat, wordt verspreid naar de werkstations uitgaande van de veronderstelling dat die software ongewijzigd is. Dat moet je dan wel controleren. Zoiets noemen we een 'integriteitscontrole' en al in de zomer van 2003 (Pictogram 3, 2003) verscheen in de Pictogram een column over Stealth, een systeem waarmee op slimme wijze de integriteit van software op (bijvoorbeeld) installatieservers kan worden gecontroleerd. Er was

Here is your password:

```
Password: ^6Bvld#*
Sentence: Beter een vogel in de hand
          ^ 6    B   v    l  d  #   *
```

You provided the following information:

Sentence: Beter een vogel in de hand
Minimal sentence Length: 6

ondanks dat helaas geen sprake van een actieve integriteitscontrole op de installatieservers.

Uitdaging

Een andere goede ingang voor hackers zijn passwords. Zodra je iemands password hebt, ben je binnen, en veel van de RUG-werkstations hebben de (vanuit beveiligingsoogpunt) vervelende eigenschap dat ze intern bijhouden welke passwords er zoal zijn gebruikt. Dus, als ik hacker ben en ik ontdek iemands password dan heb ik in no-time ook de passwords van andere gebruikers op het systeem dat door de gebruiker waarvan ik het password heb weten te achterhalen wordt gebruikt. Wedden dat daar ook het 'administrator password' bijzit? Zou het administrator password soms ook werken op andere systemen? Drie keer raden....

Ach, passwords. Hoe lang doet een hacker er nou over om een password te vinden als-ie de versleutelde versie heeft (zelfs wanneer dat een sterke versleuteling is zoals een sha1sum hash)? Als uw password uit zes letters bestaat, doet een hacker er gemiddeld een paar minuten over om uw password te achterhalen. Daar kun je op wachten.
Als je ook cijfers gebruikt wordt het iets beter: zo'n half uur zoeken per password. Eigenlijk wordt het voor de hacker pas echt een beetje een uitdaging wanneer de passwords ook andere tekens dan letters en cijfers bevat: wanneer zowel letters, hoofd- en kleine letters, als cijfers als leestekens worden gebruikt, is een hacker er gemiddeld een dag of twee mee zoet om een password van zes tekens te achterhalen. Beantwoord nu voor uzelf de vraag: in welke categorie valt uw password?

Langere passwords zijn veiliger dan korte. Een password van acht karakters is al weer een stuk veiliger dan een password van zes. En, geachte lezer, ook over passwords hebben we het al eens in Pictogram gehad (zie bijvoorbeeld Pictogram 2, 2005): een sterk password gebruiken is eenvoudiger dan je zou denken.

Roekeloos rijgedrag

De verleiding is groot om steeds meer technisch geweld in te zetten om de risico's te verkleinen. Een heilloze weg. Techniek is in dit verband niet meer dan een hulpmiddel. Een veiligheidsgordel en airbags zijn mooi, maar het voorkomen van onveilige situaties werkt waarschijnlijk beter. Of je van de onveiligheid bewust zijn en er naar handelen. Ik verwacht dat roekeloos rijgedrag van 2CV-chauffeurs minder voorkomt dan roekeloos rijgedrag van chauffeurs in 'sportieve' autotypes. De 2CV-chauffeur kijkt wel uit!

Naast technische ondersteuning om RUGnet veilig te houden, is de inzet van de gebruikers ervan zeker zo belangrijk. In ieder geval is dat zo in een zo open omgeving als een universiteit. Wetenschap is een sociaal proces, en die gedachte ligt ook ten grondslag aan onze Acceptable Use Policy (AUP): een open netwerk is alleen mogelijk wanneer iedereen meehelpt dat netwerk open en veilig te houden. Afschuiven van 'de beveiliging' naar 'het systeembeheer' is flauw en getuigt van een bedenkelijk verantwoordelijkheidsgevoel.

Security mentaliteit

Het wachten is op het volgende incident van aanzienlijke omvang. Wat kunnen we doen om dat te bestrijden? Dat is het aardige van incidentbestrijding: je weet van tevoren niet wat het volgende incident zal zijn; je weet alleen dat er een volgend incident zal komen. Binnen de Security Kerngroep verschuift de aandacht dan ook steeds meer naar incident-types (bijvoorbeeld getypeerd naar omvang) en steeds minder naar reactief beleid (hoe moeten we met dit specifieke incident in de toekomst omgaan).
Maar uiteindelijk is het binnen onze universiteit niet zo dat de Security Manager of de Security Kerngroep veiligheid kan afdwingen. Nogmaals: we zijn geen bank. Security is een mentaliteit en het nastreven van een veilige werkomgeving en een veilig RUGnet is evenals de wetenschap zelf een sociaal proces: 'Be part of the solution, not part of the problem'.

Frank Brokken
(zeer sociaal)