Frank Brokken / f.b.brokken@rug.nl

De vesting Bourtange

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.

In Oost-Groningen ligt Bourtange, een prachtige oude vesting die nog nooit door de vijand is veroverd. De vesting Bourtange is zeker de moeite van een bezoekje waard. Dat geldt vooral voor wie geïnteresseerd is in het onderwerp beveiliging.

Het leuke van Bourtange is dat de vesting alle kenmerken heeft van een goede verdediging. En het heeft gewerkt, kennelijk. Laten we eens wat kenmerken op een rijtje zetten.

Wie z'n zaakjes wil beveiligen, doet er goed aan niet over één nacht ijs te gaan. Het kan zijn dat een aanvaller een verdedigingsvorm weet te passeren, maar het wordt lastig om ongemerkt of zonder verliezen van betekenis een serie verdedigingslinies te doorbreken.

In Bourtange is dit principe goed terug te vinden: er is niet één slotgracht, maar er zijn er meerdere. De vijand moet ze allemaal passeren voordat de kern van de vesting uiteindelijk is bereikt. En dat is lastig: elke slotgracht moet opnieuw worden gedempt, of worden overbrugd en de kans dat je dat ongemerkt lukt is voor de eerste gracht al niet groot, maar praktisch nul wanneer alle grachten moeten worden gepasseerd.

Daarnaast put het passeren van een slotgracht je hulpmiddelen enigszins uit: hoeveel ton dempingsmateriaal en hoeveel bruggen heb je als vijand tot je beschikking? Een gelaagde verdediging is dan ook een goede manier om het leven van de vijand extra moeilijk te maken. *Defense in depth* wordt dat ook wel genoemd.

Moderne misser

Maar goed, de vijand kan zich natuurlijk specialiseren in het bouwen van bruggen. Voor zo'n vijand is een brug niet snel te ver, natuurlijk. De ontwikkelaars van Bourtange wisten dat ook, en hebben daar ook iets op gevonden. Een principe dat ook nu nog op ruime schaal in alledaagse situaties terug wordt gevonden: 'wed niet op één paard', 'pleeg geen monocultuur' zijn bekende adviezen.

In de wereld van de beveiliging vind je dat terug als de toepassing van het principe van de gevarieerde beveiliging. Bourtange heeft niet alleen slotgrachten, maar er zijn ook wallen opgeworpen en de bastions (de 'taartpunten') steken zodanig naar buiten dat de verdediging een aanval vanaf meerdere posities kan proberen te pareren.

Een bekend principe dat ook bij de moderne auto's wordt toegepast: auto's hebben niet alleen veiligheidsgordels, maar ook airbags, kreukelzones, ABS-systemen en wat al niet meer. Variatie in beveiliging werkt. Als de ene methode de vijand niet tegenhoudt, dan doet de andere methode dat wel.

Uiteraard zijn de bomenrijen op de vlakke stukken tussen de wallen een moderne misser, die waarschijnlijk meer het gevolg is van tegenwoordige ecologische overwegingen dan van verdedigingstechnische: je bent wel gek als je het de vijand op die manier makkelijk maakt om niet alleen ongezien te naderen, maar ook nog eens mogelijkheden biedt om de bomen als schild te gebruiken.

Beperkte toegang

Maar goed. Bourtange biedt de verdediger nog meer. In veel gevallen zal de verdediging van zo'n vesting op een laag pitje hebben gestaan. Lang niet altijd zullen de wallen bezet zijn geweest met zwaar bewapende soldaten en dergelijke. Hoe verdedig je de vesting in tijden van relatieve vrede?

In zo'n situatie probeer je als verdediger controle te houden over wat er wel en niet de vesting in komt. De toegang tot de vesting is niet onbeperkt mogelijk: er zijn maar een paar toegangswegen tot de vesting, en die toegangswegen worden actief gecontroleerd door wachtposten die zich bewust zijn van het belang van hun functie.

Hoe boeiend Bourtange ook is, het meest interessante ervan vind ik eigenlijk nog wel dat

het helemaal niet gaat om Bourtange. Wie naar de kaart van Noord-Nederland kijkt, ziet dat er allerlei vestingen aan de grens zijn gebouwd: Nieuweschans, Bourtange, Coevorden. Ze zijn daar gebouwd om iets heel anders dan zichzelf te verdedigen. En wat is dat dan? Juist: het 'Pronkjewail in Golden Raand': Grönnen, oftewel Groningen.

Opmerkelijk in dit verband is dat er tussen Bourtange en Coevorden eigenlijk geen verdedigingswerken zijn geconstrueerd. Dat was ook niet nodig: dat hele gebied was voorzien van één groot moeras waarlangs geen leger kon passeren. Een natuurlijke verdedigingslinie is ook een verdediging, en vaak een zeer effectieve.

Computervesting

Mooi hè? Zo'n verhaal over een middeleeuwse vesting. Het aardige is dat de principes die in de middeleeuwen al bekend waren, ook nu nog steeds bij de beveiliging van onze computers worden toegepast.

Je kunt er iets van leren: wie een virusscanner heeft geïnstalleerd, moet niet denken dat zijn of haar computer daarmee veilig is: er is geen defense-in-depth, geen variatie in verdediging en er zijn wie weet hoeveel toegangsroutes tot de informatie die in de computer is opgeslagen. En waarschijnlijk weet u ook niet hoeveel toegangsroutes er eigenlijk zijn tot de informatie in uw computer: tien tegen één dat u geen 'alerte wachtpost' bent die controleert wie en wat er zoal in en uit uw 'computervesting' gaat.

Het kan beter. Behalve een virusscanner helpt een intelligente gebruiker natuurlijk ook wel enigszins. Iemand die niet elke attachment maar klakkeloos opent. Wim Liebrand, oud-directeur van het (toen nog) Rekencentrum en nu directeur SURF, vertelde mij onlangs dat er allerlei e-mail namens hem wordt verspreid waarin Viagra wordt aanbevolen. Hij bezweert mij dat hij niet de afzender is. Ik geloof dat wel. Mail versturen namens iemand anders is een fluitje van een cent en daarmee wordt het ook riskant om attachments van e-mail die kennelijk door vrienden of collega's is verstuurd, zo maar te openen.

Zelfde principes

Het kan eenvoudig beter: elektronische handtekeningen zoals geboden door GPG en PGP of e-mailcertificaten maken het praktisch onmogelijk om namens iemand anders e-mail te versturen.

Het kan nog beter: een firewall die met een *default deny policy* is geconfigureerd, is te prefereren boven een firewall die elke keer dat je een nieuwe website opzoekt, vraagt of dat wel mag. Een tamelijk onzinnige instelling. Default deny verdient de voorkeur, en dat is niet dat *by default* alle verkeer wordt geblokkeerd, maar dat vanuit het internet geen verbindingen met uw computer kunnen worden geïnitieerd. Dat is heel andere koek.

Wanneer u er dan ook nog eens voor zorgt dat de programma's op uw computer up-to-date zijn (en niet alleen de laatste *service pack* is geïnstalleerd), dan zijn we een eind op weg om principes die al honderden jaren met succes zijn toegepast in de vestingbouw ook hun vruchten te laten afwerpen in de alledaagse beveiliging van uw computer.

Frank B. Brokken
'De verdediging is de beste aanval'

- GPG en PGP:
  http://enigmail.mozdev.org
  www.rug.nl/cit/security/documenten/e-mailbeveiliging
- e-mailcertificaten:
  www.startssl.com
  www.goingware.com/encryption