Beveiliging tegen indirect menselijk falen

Marcel Spruit

Traditioneel richt informatiebeveiliging zich met name op bedreigingen die direct kunnen leiden tot een verstoring. Dit geldt ook voor bedreigingen die voortkomen uit menselijk falen. In bepaalde omstandigheden kunnen menselijke handelingen echter tot een verstoring leiden, terwijl er geen sprake is van een duidelijke fout of overtreding. De vraag is hoe men zich tegen dit soort handelingen kan beveiligen.

INLEIDING

Informatiebeveiliging richt zich op het beschermen van informatiesystemen, en de informatie daarin, tegen allerlei bedreigingen door het implementeren van beveiligingsmaatregelen. De bedreigingen, waartegen informatiesystemen en informatie beschermd moeten worden, zijn zeer divers. We kunnen bijvoorbeeld denken aan natuurgeweld, stroomstoringen, computerstoringen, 'bugs', vergissingen, fraude, en nog veel meer. Uit onderzoek [1] blijkt dat de meeste beveiligingsincidenten direct of indirect veroorzaakt worden door menselijk falen. Dit kan zowel betrekking hebben op onopzettelijk falen, zoals bijvoorbeeld het per ongeluk wissen van een bestand, als op opzettelijk falen, zoals het plegen van fraude.

Een belangrijk onderdeel van informatiebeveiliging is het selecteren van beveiligingsmaatregelen. Hiervoor wordt veelal gebruik gemaakt van risicoanalyse [2], waarmee men kan onderzoeken welke maatregelen getroffen moeten worden om de risico's voor de informatievoorziening tot een aanvaardbaar niveau terug te brengen. Het denkschema dat hierbij gehanteerd wordt, is getoond in Figuur 1. In eerste instantie wordt met preventieve beveiligingsmaatregelen getracht te voorkómen dat bepaalde bedreigingen tot een verstoring leiden. Mochten deze maatregelen niet afdoende zijn, dan wordt met repressieve beveiligingsmaatregelen getracht om de schade te beperken, of zelfs te voorkómen.

Figuur 1: Van bedreiging tot schade.

Voor veel bedreigingen kunnen rechtoe-rechtaan beveiligingsmaatregelen gevonden worden, die effectief werkzaam zijn tegen de betreffende bedreigingen. Zo kan men zich bijvoorbeeld goed beveiligen tegen uitval van de netspanning, door gebruik te maken van een noodstroomvoorziening. Ook tegen veel vormen van menselijk falen kan men zich op een dergelijke wijze beveiligen (zie Figuur 2). Men kan bijvoorbeeld denken aan de maatregel functiescheiding die ingezet wordt tegen fraude.

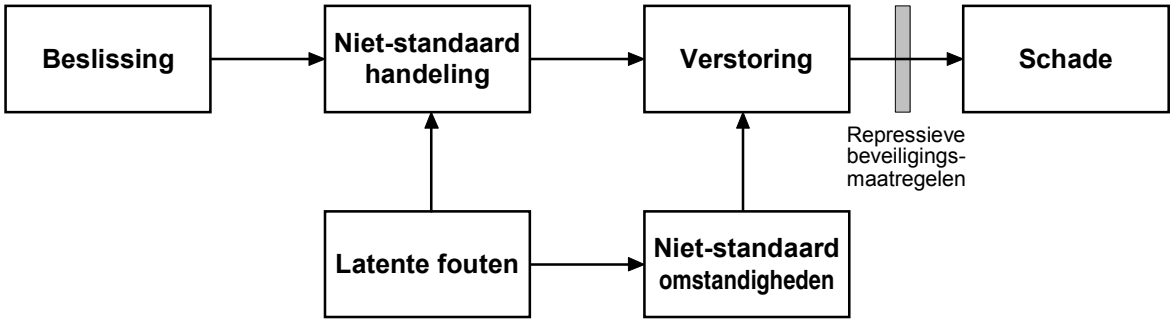
Figuur 2: Van menselijke fout tot schade.

Er zijn echter situaties waarin een bepaalde handeling in specifieke omstandigheden leidt tot een verstoring, en zo tot schade, terwijl de betreffende handeling op zichzelf niet herkenbaar is als een fout of overtreding. Het is zelfs mogelijk dat de handeling binnen het werk volstrekt normaal is, maar desalniettemin in een bepaalde (ongelukkige) samenloop van omstandigheden tot een verstoring leidt.
De vraag rijst dan welke beveiligingsmaatregelen getroffen kunnen worden om dit soort verstoringen tegen te gaan. We zullen daarvoor eerst kijken hoe menselijke handelingen indirect tot verstoringen kunnen leiden (indirect falen), om vervolgens te kijken naar de maatregelen die men kan treffen.

INDIRECT FALEN

In Figuur 3 is geschematiseerd dat een beslissing in bepaalde omstandigheden kan leiden tot schade. Het schema is gebaseerd op het incident-model van Groeneweg [3]. In eerste instantie leidt een bepaalde beslissing tot een handeling, die (meestal) afwijkt van het normale patroon (niet-standaard handeling). In samenloop met bepaalde omstandigheden, die eveneens afwijken van het normale patroon (niet-standaard omstandigheden), zal de niet-standaard handeling leiden tot een verstoring. De meeste andere combinaties van handelingen en omstandigheden zullen niet tot een verstoring leiden. De niet-standaard omstandigheden kunnen op hun beurt veroorzaakt worden door andere niet-standaard handelingen, maar ook door toevallige gebeurtenissen, zoals bijvoorbeeld blikseminslag, overstroming, etcetera.

Belangrijk is dat een bepaalde beslissing slechts in een bepaalde samenloop van omstandigheden zal leiden tot schade. Dat maakt het moeilijk om de betreffende beslissing te herkennen als potentieel gevaarlijk.



Figuur 3: Indirect falen.

Aan de hand van een voorbeeld zullen we het schema in Figuur 3 toelichten:

> *Iemand moet een offerte voor een belangrijke opdracht vóór de volgende ochtend afmaken, maar om 5 uur 's middags is de offerte nog lang niet af. Overwerken op kantoor kan niet, want zijn vrouw is niet thuis en de oppas is ziek. Hij moet dus 's avonds thuis zijn, om op de kinderen te passen. Gezien het belang van de offerte, dringt de baas er op aan dat hij het stuk dan maar thuis afrondt. Om dat te kunnen doen, neemt hij alle gegevens die hij nodig heeft op floppy mee naar huis. Helaas is hij op weg naar huis het slachtoffer van een zakkenroller, die zijn portefeuille steelt, met daarin de betreffende floppy. Later blijkt dat de gegevens op de floppy uiteindelijk bij een concurrent terechtgekomen zijn, die daarmee in staat was om de opdracht in de wacht te slepen.*

Hoe kon de beslissing om thuis te gaan overwerken (*de beslissing*), er toe leiden dat een belangrijke opdracht naar een concurrent ging (*de schade*)? In eerste instantie zijn er in de organisatie een aantal probleempunten aanwijsbaar, zoals de tijdsdruk en het ontbreken van goede thuiswerkfaciliteiten (*latente fouten*). Toen door tijdsdruk en een zieke oppas een uitzonderlijke situatie was ontstaan, waarin de baas er op aandrong om thuis over te werken (*niet-standaard omstandigheden*), toen nam de man vertrouwelijke gegevens mee naar huis, terwijl hij daar niet aan gewend was (*niet-standaard handeling*). De man had pech dat hij juist dan een zakkenroller tegenkwam (*niet-standaard omstandigheid*). De zakkenroller profiteerde van de situatie door de portefeuille, met daarin de belangrijke gegevens op floppy, te stelen (*de verstoring*). Gebruik van encryptie had de schade nog kunnen beperken (*repressieve beveiligingsmaatregel*). Maar de gegevens op de floppy waren niet vercijferd, zodat de schade een feit was.

BEVEILIGING TEGEN INDIRECT FALEN

In het voorbeeld bleek een logische beslissing, namelijk om thuis over te werken, te kunnen leiden tot een ernstig incident, namelijk het verlies van een belangrijke opdracht. Wat kan in een dergelijke situatie gedaan worden om dit soort problemen te voorkómen? In de klassieke aanpak wordt eerst een schuldige gezocht en gestraft. Vervolgens richt men zich op het verbeteren van het beveiligingsbewustzijn van de medewerkers en daarnaast worden strengere beveiligingsmaatregelen getroffen. Echter, in het voorbeeld is geen enkele reden om te veronderstellen dat de man of zijn baas onzorgvuldig gehandeld zouden hebben. De hoofdrolspelers waren te goeder trouw en konden niet voorzien wat de reikwijdte van hun beslissingen was. Om een dergelijke ongelukkige gang van zaken te voorkomen, ligt het dan ook niet voor de hand om het beveiligingsbewustzijn van deze personen te verbeteren, want daar was waarschijnlijk niets mis mee. Ook het zonder meer invoeren van zware beveiligingsmaatregelen, om alle mogelijke niet-standaard omstandigheden te voorkómen, is niet de meest geschikte oplossing. In het algemeen kunnen niet-standaard handelingen en omstandigheden in zo veel verschillende combinaties voorkomen dat het ondoenlijk is om ze allemaal te identificeren en te elimineren. Toch richt de traditionele beveiligingsaanpak zich veelal juist wel hierop. Met name na het optreden van een beveiligingsincident worden de daaraan ten grondslag liggende niet-standaard handelingen en omstandigheden gezocht, waartegen nieuwe beveiligingsmaatregelen geïmplementeerd worden. Effectiever is het echter, om de problemen bij de bron aan te pakken, namelijk door het elimineren van latente fouten. In het voorbeeld waren dit de tijdsdruk en het ontbreken van goede thuiswerkfaciliteiten. Deze fouten kunnen met eenvoudige maatregelen geëlimineerd worden:

- De tijdsdruk: Meer personeel, minder opdrachten, meer thuiswerken, of een betere werkverdeling kunnen de tijdsdruk zodanig verminderen dat overwerk niet, of in mindere mate, nodig is.
- Het ontbreken van goede thuiswerkfaciliteiten: Door een goede thuiswerkplek te creëren met een beveiligde online-verbinding tussen huis en kantoor, is het niet meer nodig om

met gegevens over straat te sjouwen. Bovendien kan dan ook niet meer de situatie ontstaan dat tijdens het thuiswerken blijkt dat nog andere gegevens meegenomen hadden moeten worden.

De genoemde fouten zijn slechts een paar mogelijkheden uit een scala van potentiële latente fouten. Door Groeneweg [3] worden de volgende onderwerpen onderkend waarin latente fouten op kunnen treden:

- het ontwerp van de installatie, apparatuur en gereedschap;
- de kwaliteit van de apparatuur en gereedschap;
- het managen en het uitvoeren van het onderhoud;
- het dagelijks onderhoud van de werkplek;
- de fysieke werkomstandigheden op de werkplek, zoals temperatuur, lawaai, etcetera;
- de begrijpelijkheid, juistheid, aanwezigheid en uitvoerbaarheid van procedures;
- de communicatie tussen werknemers, afdelingen en bedrijfsonderdelen;
- het management van tegenstrijdige doelen, zoals beveiliging versus productie;
- de structuur van de organisatie waarin moet worden gewerkt;
- de geoefendheid en ervaring van de werknemers.

Als voor al deze onderwerpen grondig aandacht besteed is aan het opsporen, bespreken en elimineren van latente fouten, dan wordt voorkómen dat werknemers in omstandigheden gebracht worden, waarin ze, wellicht zonder het te beseffen, gedrag gaan vertonen dat vanuit het oogpunt van beveiliging ongewenst is.

Vervolgens kunnen als extra ‘vangnet’ repressieve beveiligingsmaatregelen getroffen worden om er voor te zorgen dat als er toch een verstoring optreedt deze niet escaleert tot een incident met schade. Voorbeelden van repressieve maatregelen zijn:

- encryptie;
- backup;
- uitwijk;
- verzekeren.

CONCLUSIE

In het algemeen kunnen we stellen dat veel informatiebeveiligingsprogramma’s zich teveel richten op de bedreigingen die direct tot een verstoring kunnen leiden. Dit geldt ook voor bedreigingen waarbij menselijk falen een rol speelt. Een belangrijke groep van bedreigingen wordt dan echter over het hoofd gezien, namelijk handelingen die op indirecte wijze tot een verstoring kunnen leiden. Het identificeren en elimineren van mogelijke oorzaken van dit soort bedreigingen is geen eenvoudige opgave, maar wel noodzakelijk. Een adequaat beveiligingsprogramma dient rekening te houden met alle relevante bedreigingen, dus ook de bedreigingen die gevormd worden door indirect falen.

REFERENTIES

1 M.E.M. Spruit en M. Looijen, *IT security in Dutch practice*, Computers & Security, Vol.15, No.2, 1996, p. 157

2 Nederlands Genootschap voor Informatica, Afdeling Beveiliging, *Risicoanalyse en risicomanagement*, Kluwer Bedrijfswetenschappen, Deventer, 1992

3 J. Groeneweg, *Controlling the controllable*, DSWO Press, Leiden, 1996