Whitepaper beveiliging digitaal toetsen

Teelen Kennismanagement

VERSIE
1.0

AUTEUR
ir. A. Bosma (toetssysteemontwikkelaar)
mw. drs. J. Soeting (onderwijskundige/toetsdeskundige)
Teelen B.V.

DATUM
28 februari 2014

Inhoudsopgave

1. Inleiding 2

2. Toetssystemen en informatiebeveiliging 2

3. Bedreiging, kwetsbaarheid en risico 3
3.1 Wat verstaan we eronder? 3
3.2 Bedreigingen en kwetsbaarheden 4
3.3 Risicoanalyse 5

4. Beveiligingsmaatregelen 6

5. Voorbeelden van concrete maatregelen 7
5.1 Secured browser (kiosk mode) 7
5.2 Tablets 7
5.3 Secured Test Environment 7
5.4 Werkplekinrichting 8
5.5 Goede controle op de identiteit van de kandidaat 8
5.6 Goede surveillance 9
5.7 Identiteit van de werkplek 9
5.8 Netwerk 9

6. Continue analyse en verbetering 10
6.1 Blijf alert 10
6.2 Bewustwording 10
6.3 Ineffectieve maatregelen 10

Beveiliging is zowel bij de traditionele toetsafname als bij digitaal toetsen een punt van zorg, en dat is terecht. Fraudeurs zijn zeer creatief in het bedenken en toepassen van nieuwe technieken om een voldoende voor een examen te halen, vooral als het belang van het examenresultaat groot is. Door de snelle vooruitgang en bredere toegankelijkheid van de techniek zijn geavanceerde fraudemogelijkheden in korte tijd binnen ieders bereik gekomen. De beveiliging van uw toetsomgeving heeft daarom voortdurend aandacht en onderhoud nodig.

Het is zonder meer mogelijk om een goed beveiligde digitale toetsomgeving in te richten, maar dit gaat niet vanzelf. Informatiebeveiliging is niet alleen een zaak van techniek, maar vooral van mensen. Als informatiebeveiliging belangrijk is voor uw organisatie, is het nodig om aandacht te geven aan beide aspecten. Door inzichten uit de informatiebeveiliging toe te passen, voorkomt u dat u kiest voor ineffectieve maatregelen. Hierdoor zal de kwaliteit van de beveiliging op het gewenste niveau komen te liggen.

Dit whitepaper bevat een overzicht van voor toetssystemen relevante inzichten over informatiebeveiliging en laat zien hoe deze gebruikt kunnen worden voor ontwerp en implementatie van effectieve beveiligingsmaatregelen rond digitale toetsing.

1. Inleiding

Horrorverhalen over beveiligingsincidenten worden tegenwoordig breed uitgemeten in de media. Bedreigingen zoals *Denial of Service attacks* van botnets, spionerende overheden, slecht beveiligde websites en bendes die proberen te infiltreren in het internetbankieren, passeren vrijwel dagelijks de revue. Mede daardoor worden technische bedreigingen zwaar ingeschat bij de introductie van digitaal toetsen. Op internet kwamen we het volgende devies tegen: "*Ga nooit digitaal examineren. Het is vragen om problemen, die je niet in de hand kunt hebben*". Door problemen die zich in het verleden met digitaal toetsen hebben voorgedaan, is deze kritische houding niet verwonderlijk. Vaak blijkt echter dat (dezelfde) problemen met een vergelijkbaar risico bij een examen op papier wel worden geaccepteerd, omdat we daarmee vertrouwd zijn. Identiteitsfraude bijvoorbeeld, is geen fenomeen exclusief voor digitaal toetsen. De overgang naar een digitale toetsomgeving kan identiteitsfraude wel faciliteren. En het risico wordt groter als de investering in de digitale toetsomgeving grote kostenbesparingen op andere punten met zich mee moet brengen.

Wat opvalt is dat veel mensen lijken te verwachten dat beveiligingsproblemen als sneeuw voor de zon verdwijnen door technische bling-bling te installeren of er een certificaat op te plakken. Technische maatregelen treffen tegen *alle* mogelijke bedreigingen blijkt echter ontzettend duur te zijn. Bovendien kan dit er toe leiden dat het systeem in de praktijk onbruikbaar is. Voor het uiteindelijke resultaat is de organisatie rond het toetsen zeker zo belangrijk. De zwakste schakel in de beveiliging is namelijk de mens.

Digitale toetsing kan in veel gevallen juist voorkomen dat er fraude gepleegd wordt. Wanneer de toegestane boeken digitaal ingezien kunnen worden, weet je zeker dat het om het juiste boek gaat, en dat er geen aantekeningen en spiekbriefjes in verstopt zitten. Een groot verschil tussen papier en digitaal is wel dat fraude met papier meestal fysieke sporen achter laat, zoals bij het openen van een verzegelde envelop en het aanpassen van antwoorden. Digitale fraude kan anoniem gepleegd worden, op afstand. Dat maakt het op heterdaad betrappen van een fraudeur lastig.

Ten slotte moeten we ook het recht op privacy van de kandidaat niet uit het oog verliezen. Toetsresultaten vallen in het algemeen niet in de hoogste risicoklasse, maar het zijn wel vertrouwelijke gegevens. De kandidaat verwacht terecht dat er zorgvuldig met deze gegevens wordt omgesprongen.

2. Toetssystemen en informatiebeveiliging

Natuurlijk moet een toetssysteem afdoende beveiligd zijn tegen misbruik, maar als we goed kijken naar wat er nu eigenlijk beveiligd moet worden, dan

is dat niet het systeem (de kluis; het middel), maar de informatie (de sieraden; het doel). Bij informatiebeveiliging draait het drie belangrijke aspecten.

Beschikbaarheid. Kan ik de informatie gebruiken wanneer ik die nodig heb? Als de stroom uitvalt, of als het systeem zo traag reageert dat er niet mee te werken valt, dan is aan de beschikbaarheidseis niet voldaan.

Integriteit. Is de informatie actueel en correct? Voor de kwaliteit van een toetsresultaat is het essentieel dat de gegeven antwoorden afkomstig zijn van de juiste kandidaat. Ook moet de kandidaat de juiste toets ontvangen waarin de juiste vragen zijn opgenomen.

Vertrouwelijkheid. Krijgen alleen geautoriseerde personen toegang tot de informatie? Privacybescherming enerzijds en vertrouwelijkheid van de toetsgegevens anderzijds zijn erg belangrijk. Bedenk dat informatie over een toets mondeling of digitaal gedeeld kan (en zal) worden. Ook via systemen die in een andere invloedsfeer liggen, zoals Facebook en Twitter.

Het is essentieel om vanaf het begin voor alle drie aspecten de noodzakelijke beveiligingsmaatregelen mee te nemen in het ontwerp van een digitale toetsomgeving. Wanneer pas na realisatie blijkt dat gerealiseerde service levels in de praktijk onvoldoende zijn, kost dit veel meer tijd en geld. Andersom: investeringen in maatregelen die achteraf overbodig blijken te zijn, verdienen zich nooit terug.

3. Bedreiging, kwetsbaarheid en risico

3.1 Wat verstaan we eronder?

Hieronder ziet u vier belangrijke termen binnen informatiebeveiliging.

Bedreiging	een gebeurtenis of persoon die gevaar oplevert
Kwetsbaarheid	een aspect waar een bedreiging op kan inwerken of gebruik van kan maken
Incident	een gebeurtenis die daadwerkelijk een probleem en/of schade oplevert
Risico	de kans dat een incident plaatsvindt maal de schade die dat veroorzaakt

Bijvoorbeeld: een hacker is de bedreiging, de kwetsbaarheid is een verouderd besturingssysteem. Zonder de kwetsbaarheid leidt een bedreiging niet tot een incident. Een belangrijke bedreiging voor een *toetssysteem* is een student die probeert te frauderen. Onlangs was in het nieuws dat toetsen van Cito voor geld worden aangeboden. Zodra je geld kunt verdienen met

gestolen toetsen, vormen ook criminelen ineens een serieuze bedreiging voor een toetssysteem.

Het doel van informatiebeveiliging is om het risico te beperken tot een vooraf bepaald, acceptabel niveau. Veranderingen in de buitenwereld hebben meestal invloed op het risico, want ze zorgen voor nieuwe bedreigingen en kwetsbaarheden. Wanneer je een tijd geen aandacht geeft aan beveiliging, loopt het risico vaak ongemerkt hoog op.

3.2 Bedreigingen en kwetsbaarheden

Het is belangrijk om eerst alle bedreigingen en kwetsbaarheden goed in kaart te brengen voordat maatregelen getroffen worden.

Voorbeelden van bedreigingen en kwetsbaarheden voor het aspect beschikbaarheid

- Uitval van kritische systemen
  - Stroomstoring
  - Brand
  - Water: Overstroming, lekkage, koffie
  - Internetstoring (graafwerkzaamheden, afsluiting door provider)
- Achterstallig softwareonderhoud
  - Verlopen certificaat
  - Verlopen licentie
- Software update
  - Onvoldoende getest
  - Verkeerde timing van de update (een update van een virusscanner of van het besturingssysteem tijdens een examen)
- Technische drempel om de toets te kunnen maken is te hoog
  - Ergonomie
  - Handicap van de kandidaat
  - Licht: door zonlicht is niet van het beeldscherm te lezen
  - Klimaat: te warm of te koud om te werken
  - Werkplek voldoet niet aan vereisten
- Overbelasting van de netwerkinfrastructuur
  - Aanval door hackers
  - Samenloop van omstandigheden (multimedia gebruik in onderwijs tijdens examen)
- Configuratiefouten
  - Firewall staat niet open
  - De toets is niet beschikbaar voor de kandidaten
  - Het afnamewachtwoord is gewijzigd, maar niet bekend bij de surveillant

Voorbeelden van bedreigingen en kwetsbaarheden voor het aspect integriteit

- Identiteitsfraude
  - Sturen van een lookalike
  - Gebruik van een vals identiteitsbewijs

    - Wisselen van werkplek
- Communicatie (of samenwerken) tijdens de toets
    - Gebruik van smartphones, walkie-talkies.
    - Studiemateriaal, spiekbriefjes, google
    - Uitwisselen van aantekeningen of antwoordformulieren
    - Afkijken
- De verkeerde toets staat klaar
- Onbevoegden veranderen toetsvragen
- Fraudeurs die examenresultaten willen veranderen
- Surveillanten die onvoldoende zijn geïnstrueerd of gescreend

Voorbeelden van bedreigingen en kwetsbaarheden voor het aspect vertrouwelijkheid:
- Fraudeurs die een examen vooraf willen inzien
- Met behulp van de camera van een smartphone kunnen toetsvragen van het beeldscherm doorgegevens worden aan personen buiten de examenzaal
- Hackers stelen persoonsgegevens om door te verkopen aan de hoogste bieder
- Journalisten die op zoek zijn naar examenresultaten van bekende Nederlanders

3.3 Risicoanalyse

Op basis van een risicoanalyse worden de kwetsbaarheden aangewezen waar maatregelen noodzakelijk zijn, omdat blijkt dat het risico onacceptabel hoog is. Maatregelen die de gevolgen van een incident beperken, zorgen vaak ook voor een vermindering van de risico's. Het lukraak implementeren van enkele maatregelen zonder voorafgaande analyse, leidt vaak niet tot een verlaging van het risico. De ketting is nu eenmaal zo sterk als de zwakste schakel.

Het belangrijk om ook de samenhang van de risico's te beoordelen. Het netto rendement van een kostbare 99.99% uptime garantie (beschikbaarheid) is nihil wanneer tijdens het examen blijkt dat de verkeerde toets klaarstaat (integriteit). In dit geval zijn risico's rond beschikbaarheid mogelijk te zwaar ingeschat en zijn de andere aspecten onderbelicht gebleven. Vergeet daarbij niet dat het altijd mogelijk is om een keer pech te hebben. Meteen na een incident worden de risico's vaak veel hoger ingeschat dan ze zijn. Als een tijdlang geen incidenten hebben plaatsgevonden, worden de risico's onderschat. Organisaties komen daardoor vaak in een ineffectieve cyclus van overdreven beveiligingsmaatregelen terecht, die langzaam verwateren waardoor het risico gestaag toeneemt tot het volgende serieuze incident zich aandient.

4. Beveiligingsmaatregelen

Beveiligingsmaatregelen moeten altijd bijdragen aan het verminderen van de onderkende risico's. Bij iedere maatregel moet de afweging gemaakt worden of de kosten van een maatregel opwegen tegen de schade die onderkende risico's kunnen veroorzaken. Onder de noemer kosten vallen ook indirecte kosten, zoals bijvoorbeeld verminderd gebruiksgemak en administratieve rompslomp.

De bedreigingen in een omgeving waar digitale toetsen worden afgenomen en in de traditionele examenlocaties zijn met name op het aspect beschikbaarheid verschillend. Wanneer het toetssysteem niet beschikbaar is, kan het examen geen doorgang vinden en dat heeft flinke negatieve gevolgen. Stel nu eens dat de gewenste beschikbaarheid op 99,5% tijdens kantooruren wordt vastgesteld (maatregel). Dat ziet er op het eerste gezicht uitstekend uit. Helaas valt het systeem net uit op een moment dat het erg druk is (zou dat toeval zijn?). Deze storing van een half uur kan dan gemakkelijk 20% van het totaal aantal examens hebben beïnvloed, terwijl de beschikbaarheid in deze maand is nog steeds ruim 99,8%. Wanneer de storing langer duurt, krijg je soms een schadevergoeding van de aanbieder. Geld compenseert echter de gevolgen van het incident niet, waardoor de maatregel eigenlijk niet effectief is.

Zowel papier als computer bieden mogelijkheden om fraude te plegen. Een fraudeur kiest daarbij de weg van de minste weerstand. Zou een kandidaat de moeite nemen om een goed beveiligd toetssysteem te kraken, wanneer de toets op papier uit de prullenmand bij een kopieerapparaat gevist kan worden? Als organisatie veel energie steken in rechtenbeheer om het uitlekken van toetsen te voorkomen (maatregel) is zinloos wanneer de leden van de examencommissie - gefrustreerd, omdat het systeem te vaak niet beschikbaar is - via email en USBstick informatie met elkaar delen (kwetsbaarheid).

Organisaties hebben de neiging om onbereikbare doelen stellen bij de overgang van papier naar digitaal. Dat is eigenlijk heel logisch, want waarom zou je risico willen lopen? In het selectietraject blijkt dan al snel dat geen enkel systeem aan alle eisen voldoet. Zelfs wanneer er een systeem zou bestaan dat aan alle eisen voldoet, dan zullen er nog steeds incidenten optreden. Misschien is het wel gewenst een systeem te maken waarbij je altijd iemand de schuld kunt geven van een incident. Maar ook dit compenseert de gevolgen van een incident natuurlijk niet.

Een reëel te bereiken doel is om digitaal een toets af te kunnen nemen waarbij de mogelijkheden van een pc kunnen worden benut en de risico's vergelijkbaar zijn dan bij gebruik van een papieren toets. Door vooraf scenario's voor te bereiden die gebruikt kunnen worden als er iets mis gaat, beperk je de gevolgen van de risico's die je bereid bent te nemen.

Helaas is het vaak lastig om het effect van getroffen maatregel rechtstreeks te bepalen omdat je niet weet hoeveel incidenten er zouden zijn opgetreden zonder de maatregel. Dat neemt niet weg dat er feiten verzameld moeten worden, zoals het aantal, de duur en de impact van incidenten, om te kunnen controleren of (nog) aan de afgesproken doelstellingen wordt voldaan. Het is goed om het beveiligingsplan en de behaalde resultaten te vergelijken met die van soortgelijke instellingen. Via een goede analyse zijn de effectieve maatregelen dan vast te stellen. Als niet aan de doelstellingen wordt voldaan, zijn extra maatregelen noodzakelijk.

5. Voorbeelden van concrete maatregelen

5.1 Secured browser (kiosk mode)

Een veel gebruikte technische maatregel is het toepassen van een secured browser. Op de beveiligde computer zijn alleen toegestane applicaties te gebruiken. Secured browsers zijn goed te configureren voor een bepaald doel. De configuratie is echter niet erg flexibel en zonder aanvullende maatregelen kan een student vaak gemakkelijk om deze maatregel heen door de computer opnieuw te starten vanaf een USBstick of de monitor om te pluggen. Een secured browser is namelijk ontworpen voor gebruik tijdens symposia, congressen en monitors in openbare ruimtes. Daar zijn de risico's niet zo hoog als bij het afnemen van een examen. Een toegestane applicatie biedt soms achterdeurtjes om weer andere applicaties te kunnen gebruiken. Omdat de beveiliging met een secured browser alleen maar een schil legt rond de bediening van de pc, is deze aanpak ongeschikt voor omgevingen met hoge risico's. Door de secured browser onderdeel te maken van een pakket met aanvullende maatregelen zoals toezicht, firewall, fysieke bescherming kan het risico verder terug worden gebracht.

5.2 Tablets

Een tablet wordt soms gebruikt als alternatief voor een gewone computer. Kies dan in ieder geval voor apparaten die beveiligd kunnen worden (guest of kids mode). Veel tablets kunnen de rechten van een gebruiker niet of nauwelijks beperken. Wanneer een gebruiker zelf instellingen kan veranderen en applicaties kan installeren op het apparaat, zal goed toezicht noodzakelijk zijn om het fraude risico te beperken.

5.3 Secured Test Environment

Wanneer de bedreigingen serieus zijn en de risico's hoog, is de inrichting van een Secured Test Environment (STE) een goede maatregel. De examens

vinden dan plaats in een gecontroleerde omgeving, waarbij technische en organisatorische beveiligingmaatregelen zorgen voor een hoog beveiligingsniveau. Stel dat in een toetssituatie specifieke software gebruikt moet worden voor het toetsen van vaardigheden. Het moet dan mogelijk zijn om een werkplek in korte tijd zo te configureren dat alleen de toegestane software gebruikt kan worden. Soms moeten ook documenten klaargezet kunnen worden waarmee de kandidaat aan de slag kan.

De toegang tot de STE is beperkt tot bevoegde personen. Kandidaten hebben alleen toegang tijdens de toets. Wanneer een kandidaat uitgebreid toegang heeft tot apparatuur in de STE zonder toezicht, is niet te garanderen dat alleen de toegestane software wordt gebruikt. Een kandidaat moet natuurlijk wel in de gelegenheid worden gesteld om vertrouwd te raken met het gebruikte toetssysteem.

De inrichting van een STE kost veel geld, omdat er ingericht moet worden op piekcapaciteit. De bezettingsgraad van de faciliteit is vaak laag omdat examens alleen maar in korte periodes worden afgenomen. Met digitale toetssystemen is het goed mogelijk om verschillende versies te maken voor verschillende groepen, zodat de afname over een langere periode gespreid kan worden.

5.4 Werkplekinrichting

De locatie is overzichtelijk ingedeeld om effectief toezicht mogelijk te maken. Er is voldoende scheiding tussen de werkplekken om spieken of overleg onmogelijk te maken. Verder zijn de werkplekken uniform, zodat iedereen gelijke kansen heeft. Om die reden is ook het geautomatiseerd configureren van alle werkplekken voor een toets noodzakelijk. Dit voorkomt onbedoelde verschillen tussen werkplekken. Bovendien kan de ruimte meteen na afloop van een examen opnieuw voor een ander doel gebruikt worden.

Sommige organisaties staan de aanwezigheid van vloeistoffen niet toe op de examenplek, omdat een kop gemorste thee tot een storing in de apparatuur kan leiden. Een andere maatregel met hetzelfde effect is het toepassen van een waterdicht toetsenbord. Bij een lang examen draagt een kopje koffie of thee vast en zeker bij tot een goed resultaat.

5.5 Goede controle op de identiteit van de kandidaat

Het controleren van de identiteit zou bij voorkeur bij iedereen plaats moeten vinden. Doe dit in ieder geval steekproefsgewijs om te tonen dat je dit aspect serieus neemt. Het is handig wanneer het toetssysteem continu de identiteit van de ingelogde gebruiker toont, zodat de surveillant deze kan controleren. Wanneer een kandidaat kan deelnemen aan een toets met alleen een

gebruikersnaam en (standaard) wachtwoord dan is de controle op de identiteit niet hoog.

5.6 Goede surveillance

Er moet voldoende aandacht worden besteed aan de selectie en instructie van de surveillanten. Naast het controleren van de identiteit en het toezien op een goed verloop van de toetsafname, heeft surveillance (ook) de taak om als eerstelijns helpdesk/aanspreekpunt voor technische problemen te dienen. Als de problemen niet ter plekke opgelost kunnen worden, moet via een hotline de technische helpdesk ingeschakeld kunnen worden. Incidenten moeten natuurlijk met de juiste prioriteit worden afgehandeld.

Surveillance kan effectiever worden gemaakt door een afname dashboard in te zetten. De actuele configuratie van de werkplek en de status (opstarten/onjuiste inlogpoging/ ingelogd/bezig met toetsvraag x van y/toets afgerond) van de toets zijn bijvoorbeeld relevant. Andere mogelijk nuttige functies voor zo'n afnamedashboard zijn het toekennen van extra tijd (na een technisch probleem), het afsluiten van een afname, het opstellen van een proces verbaal en het toevoegen of verwijderen van kandidaten.

5.7 Identiteit van de werkplek

Een groot voordeel van internetdiensten is dat je ze altijd en overal kunt gebruiken. Dit is een kenmerk waar je bij het afnemen van toetsen niet altijd op zit te wachten. Daar wil je juist zekerheid dat de kandidaat de toets maakt in de gecontroleerde omgeving. Het gebruik van een afnamewachtwoord is een eenvoudige maatregel die meer zekerheid geeft over de gebruikte werkplek, hoewel de moderne communicatiemiddelen het eenvoudig maken om het afnamewachtwoord te communiceren, bijvoorbeeld naar een helper buiten de examenzaal. Als meer zekerheid nodig is, kunnen het beste voorzieningen in de infrastructuur van het netwerk worden getroffen.

5.8 Netwerk

Al het netwerkverkeer moet zijn versleuteld (HTTPS TLS), zodat berichten niet afgeluisterd en veranderd kunnen worden. Met een firewall is communicatie tussen werkplekken onderling en met niet noodzakelijke servers onmogelijk gemaakt. Internet is beperkt beschikbaar (whitelist) indien nodig. De noodzakelijke netwerkcapaciteit is gegarandeerd beschikbaar, en wordt evenredig verdeeld over de werkstations. Het toetssysteem accepteert alleen IP-adressen afkomstig uit de secured test environment. Houd er wel rekening mee dat zonder aanvullende maatregelen een IP-adres vrij gemakkelijk is na te bootsen. Een goede aanvulling om de te gebruiken werkplekken te beperken is het installeren

van een clientcertificaat. De toetsserver wordt dan zo ingesteld dat alleen machines voorzien van zo'n certificaat verbinding mogen maken.

6. Continue analyse en verbetering

6.1 Blijf alert

Na de realisatie van de digitale toetsomgeving is het belangrijk om bij te blijven. Beveiliging heeft altijd aandacht nodig, omdat de wereld nu eenmaal niet stilstaat. Door nieuwe technische mogelijkheden of door veranderende verwachtingen: stilstand is acheruitgang. Een versleutelingstechniek die op dit moment als betrouwbaar te boek staat kan bij wijze van spreken morgen als zwak worden betiteld omdat de techniek een sprong voorwaarts heeft gemaakt.

Je voorkomt dat (nieuwe) kwetsbaarheden grote incidenten veroorzaken door van tijd tot tijd opnieuw de risicoanalyse en de beveiligingsmaatregelen kritisch te beoordelen. Wacht dus niet tot er een groot incident optreedt, maar verzamel regelmatig beschikbare informatie en analyseer deze grondig. Vaak zijn er al signalen dat er iets mis is voordat er een serieus incident optreedt. Omdat bij misbruik van een digitaal systeem meestal geen fysieke sporen achterblijven en alle informatie gewoon aanwezig blijft, moeten de signalen die duiden op incidenten via andere bronnen worden verkregen. De analyse van toetsresultaten kan bijvoorbeeld aanleiding zijn om te vermoeden dat er iets mis is. Zorg dat signalen op de juiste plaats terecht komen door het melden (ook anoniem) gemakkelijk te maken. Laat zien dat beveiliging belangrijk is. Informatie uit het proces is een belangrijke hulp in het verder beveiligen van de digitale toetsomgeving. Kortom: neem alle signalen serieus en zorg dat incidenten op de juiste manier worden afgehandeld.

6.2 Bewustwording

Informatiebeveiliging gaat iedereen aan, en iedereen moet daaraan een bijdrage leveren. Een medewerker die bestanden van het netwerk op een USBstick zet om 's avonds nog even door te kunnen werken, neemt een beveiligingsrisico, maar is zich daarvan vaak niet bewust. Wanneer je aandacht besteedt aan beveiliging, maak je ieder geval het belang ervan duidelijk. Er zijn vele manieren om informatiebeveiliging onder de aandacht te brengen, zoals trainingen, het geven van het goede voorbeeld en het (laten) uitvoeren van penetratietesten.

6.3 Ineffectieve maatregelen

Wat in ieder geval *niet* helpt is het doorvoeren van losse, vervelende maatregelen waardoor mensen hun werk niet meer prettig kunnen doen. Het

verplicht regelmatig wijzigen van wachtwoorden is daarvan een bekend voorbeeld. Zo'n maatregel is goedkoop en gemakkelijk in te voeren, en bij een controle kan het management laten zien dat er iets aan beveiliging gedaan is. Als medewerkers het nut van zo'n maatregel niet inzien, bedenken ze spontaan een manier waardoor de beveiliging nog zwakker wordt dan die al was. De schoonmaker kan de briefjes met de wachtwoorden bijvoorbeeld zo meenemen van het beeldscherm.

Een tweede voorbeeld is het automatisch blokkeren van een account bij een aantal foute inlogpogingen. Dit is bedoeld om het raden van wachtwoorden te voorkomen. Deze maatregel maakt je echter kwetsbaar voor een scenario waarin opzettelijk enkele gebruikers de toegang tot het systeem wordt ontnomen door een fraudeur die alleen maar een aanmeldnaam weet. Als je als fraudeur in zo'n hectische situatie belt met de helpdesk voor een vergeten wachtwoord, heb je meestal binnen een minuut toegang.

Een laatste voorbeeld: omdat je geen problemen wilt door niet gepatchte besturingssystemen en virusscanners, stel je automatische updates in. Helaas leidt dit gegarandeerd tot een piekbelasting op het netwerk, wanneer alle computers op de toetswerkplekken, die een tijd niet gebruikt zijn, tegelijkertijd worden opgestart. Als de toets dan eindelijk gestart is, blijkt dat alle computers automatisch opnieuw worden opgestart, omdat de secured browser voorkomt dat de kandidaat een melding van het besturingssysteem weg kan klikken.

In een volwassen toetsomgeving moeten maatregelen dus goed zijn afgestemd op de feitelijke bedreigingen en kwetsbaarheden. Het lukraak implementeren van wat maatregelen helpt je vaak van de wal in de sloot.