

Veiligheid

Frank Brokken is security manager bij het CIT. 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.



Kom, laten we het voor de verandering eens over veiligheid hebben. Zoals iedereen vermoedelijk wel weet, al was het maar van het TV-programma 'Air Crash Investigation', heeft veiligheid in de luchtvaart een bijzonder hoge prioriteit.

Honderd checks

De meeste mensen die ik spreek, vinden het vanzelfsprekend dat veiligheid in de burgerluchtvaart zo belangrijk wordt gevonden. Ja, ongelukken gebeuren, ook in de luchtvaart, maar het hele proces om ongelukken te voorkomen en ervan te leren is in de luchtvaart toch wel bijzonder goed georganiseerd.

Een klein voorbeeldje: het is niet alleen de grote luchtvaart waarbij die veiligheid voorop staat, ook de kleine luchtvaart kan er wat van. Een van de vliegtuigen waarop ik les geef is de Piper PH-EAH.



Voordat dat vliegtuig goed en wel de lucht in gaat, worden er ruim honderd checks uitgevoerd en ook eenmaal in de lucht zijn er een kleine honderd controles die tijdens zo'n vlucht de revue passeren. Iedereen heeft wel eens gehoord van de checklist zoals die in de luchtvaart wordt gebruikt, en een stukje van zo'n checklist (inderdaad, die bij de PH-EAH hoort) zien we hier ook afgedrukt.

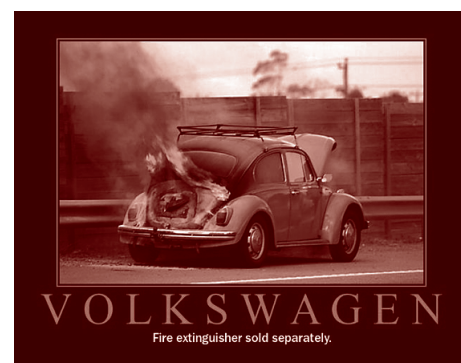
Fuel pressure	- CHECK
Idling	- CHECK
Throttle	- 1200 RPM
6. Before take-off checklist	
Seat belts	- FASTENED
Seats	- ERECTED & LOCKED
Cabin door & window	- CLOSED/LATCHED
Controls	- FREE MOVEMENT
Trims (elevator/rudder)	- SET FOR TAKEOFF
Flaps	- UP
Master/Altern. Switch	- BOTH ON
Magnetos	- BOTH ON
Electrical fuel pump	- SET/ON: nr. 1: up
Fuel pressure/quantity	- CHECK
Mixture	- RICH
Friction nut	- FASTENED
Carb heat	- COLD
Pitot heat	- ON, check warning off
Directional Gyro	- SET
Nav lights & panel lights	- AS REQUIRED
Landing light	- ON
Departure clearance	- RECEIVED
Clearance limit	- KNOWN
Departure time	- NOTED
Transponder	- CORRECT CODE & ALT
7. Runway items	
Directional Gyro	- CHECK - Runway heading
During take off run:	
Throttle	- CHECK FULL OPEN
Engine instruments	- CHECK
RPM	- 2700 RPM
Speed	- ROTATE 60 KTS
8 After take-off checklist	
-> 200" AGL	
Carb heat	- COLD
Flaps 80 KTS	- UP
Mixture	- RICH
Trim	- SET
-> trans alt or outside CTR	
Landing light	- OFF
Altimeters	- QNE (at trans alt)

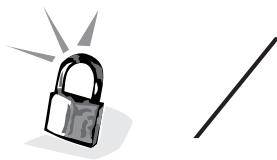
Het gebeurt niet vaak, maar soms, vlak voor het opstijgen, komen we dan bij zo'n item waarvan we zeggen 'Tja..., nou, misschien moesten we vandaag maar even niet gaan vliegen'. Een goede zaak, want om dat soort beslissingen te kunnen nemen, is het belangrijk dat je de beslispunten expliciet onder ogen krijgt en er adequaat op kunt reageren.

Uiteindelijk zijn er nogal wat items die zowel op het instrumentarium en op het functioneren van het vliegtuig als zodanig betrekking hebben en zonder checklist vergeet je dan al snel een belangrijk item waar je toch echt even aandacht aan had moeten schenken.

In de familie

Eigenlijk ken ik maar weinig situaties waarbij zo expliciet aandacht aan veiligheid wordt geschonken als binnen de luchtvaart. Zou dat te maken hebben met het feit dat wij van nature niet kunnen vliegen? Mogelijk, maar 'van nature' kunnen we ook niet autorijden en wie controleert nou voor het wegrijden het niveau





Security

van de motorolie of koelvloeistof? Ik in ieder geval niet en dat heeft me al eens bijna een verbrande motor opgeleverd. Het zal wel in de familie zitten. Zo heeft de motor van de auto van mijn vader wel eens in brand gestaan, en omdat het een VW kever was, met de motor achterin, had hij dat niet door totdat een bus achter hem toch wel erg stevig met z'n lichten begon te knippen.

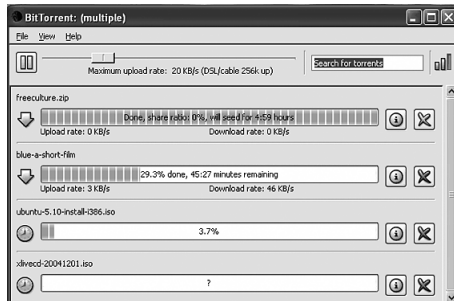
Wij kunnen ook 'van nature' niet met computers werken. Gebruiken we daar dan ook checklists? Meestal niet, hè? Er zijn wel van die grappen van het type 'Als Boeing van Microsoft zou zijn, dan kon geen enkel vliegtuig meer fatsoenlijk vliegen', maar uiteindelijk is het natuurlijk ook een beetje de verantwoordelijkheid van de individuele gebruiker wat er met zijn of haar computer gebeurt.

Copyright

Onlangs werd mij gevraagd iets te schrijven over Security voor het CIT-jaarverslag 2009. Gelukkig waren er in 2009 geen grote incidenten. Wel een aantal kleine incidenten, absoluut gezien misschien nog wel een aardig aantal. In 2009 ontvinden we zo'n 200 officiële incidentmeldingen wanneer we de herhalingen wel meetellen en niet het aantal incidenten waarbij copyrighted materiaal illegaal beschikbaar werd gesteld.

Waarom het ene wel en het andere niet? Omdat illegaal beschikbaar stellen van copyrighted materiaal toch vaak een min of meer bewuste activiteit is. Hoewel de gebruiker zich misschien niet direct realiseert dat systemen als BitTorrent niet alleen maar downloaden maar ook informatie die in je computer is opgeslagen aan derden aanbieden, is er in ieder geval op een gegeven moment door die gebruiker een bewuste beslissing genomen om BitTorrent te gaan gebruiken. En als je dan betrapt wordt op het aanbieden van copyrighted materiaal, dan is dat toch ook een beetje datgene waarom je zelf hebt gevraagd.

Dat ligt iets anders met de 200 overige officiële klachten die we hebben ontvangen. Ongeveer



30% van de ontvangen meldingen hadden betrekking op besmettingen met het Conficker-virus; ongeveer 25% van de ontvangen klachten hadden betrekking op computers die door een spam-verspreidend virus waren besmet; ongeveer 25% van de ontvangen klachten hadden betrekking op computers die als DDos (botnet) zombie konden worden ingezet.

Vaak zijn dit soort besmettingen nevenproducten van ontvangen e-mail. In de bijlage zit een attachment die besmet is met een virus of een andere vorm van kwaadaardige software. Er zijn weliswaar virusscanners, maar die detecteren alleen wat ze al kennen. Firewalls helpen in dit verband ook niets want die doen niks tegen virussen die in e-mail verstopt zitten.

Zulke virussen komen pijnloos door de firewall omdat we immers zelf de e-mail er doorheen loodsen. Uiteindelijk zijn we dan ook zelf onze ultieme virusscanner. Wanneer e-mail met attachments onze mailbox bereikt, dan weten we in ieder geval dat de virusscanner niks verdachts heeft gezien.

Attachment-checklist

Hadden we nu maar een checklist om te controleren wat we moeten doen. Maar die hebben we niet. Misschien komen we er wel met een beetje gezond verstand. Het venijn zit nou eenmaal in de staart en dat is bij e-mail altijd de attachment. Controleer daarom altijd eerst of de afzender van de e-mail eigenlijk wel bekend is. Is het een collega of andere bevriende relatie? Het is niet uitgesloten dat een virus ons via die route bereikt, maar die kans is een stuk groter wanneer we een attachment van een ons onbekende afzender ontvangen.

Een attachment doet echter op zich nog geen kwaad. Een attachment kan ons alleen kwaad



berokkenen wanneer code die erin is opgenomen ook wordt uitgevoerd, en dat kunnen we voorkomen door bijvoorbeeld .doc files niet automatisch met Word te openen maar bijvoorbeeld met WordView dat geen macros interpreteert.

Maar het blijft lastig: spreadsheet data, filmpjes en wat al niet meer kunnen als bijlage aan e-mail worden toegevoegd en al die bijlagen kunnen in principe besmet zijn. Voorzichtigheid met het openen is daarom geboden. Misschien ook even per telefoon controleren wat de kennelijke afzender ons heeft toegestuurd en waarom? Waarom is er eigenlijk een bijlage? Kan de boodschap niet gewoon in de e-mail tekst zelf worden vervat? Zo kom je toch al snel op iets van een (zeer korte) checklist:

E-mail met attachment:

- ontvangen:
 - > niet automatisch openen;
 - > verifieer de authenticiteit van de afzender.
- attachment- voorkom dat macros worden geïnterpreteerd.
- verzenden:
 - > niet doen als het niet nodig is;
 - > verstuur bij voorkeur 'kale' e-mail zonder attachments.

Zo'n 200 besmettingen: dat is een besmetting per werkdag. Wie het overkomt, baalt en de desbetreffende computer staat al snel een hele dag bij de Servicedesk. De kans dat het je overkomt is gering, maar voorkomen is beter dan genezen en door de zeer korte attachment-checklist te volgen, wordt de kans op een besmetting wel erg klein. Het lijkt de luchtvaart wel.

Frank B. Brokken, piloot
(doet z'n naam geen eer aan)