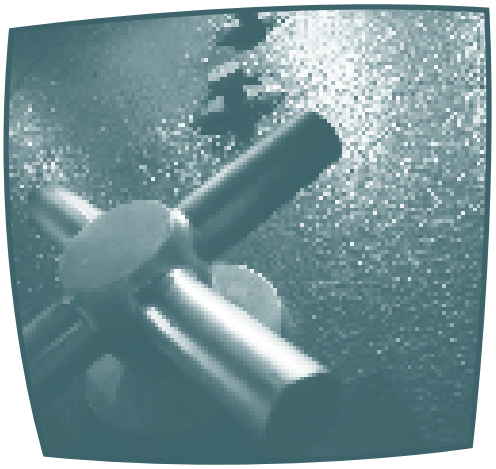
De tien belangrijkste actuele security-risico's in de IT

Mij werd gevraagd een lijst samen te stellen van de belangrijkste security-issues die de wereld van IT-bedreigen. Sommige van deze zijn typisch voor i5/OS en andere niet. Hopelijk zullen de bedreigingen, eigenlijk is 'threats' een veel mooier woord, u aan het denken zetten over uw eigen omgeving en u ertoe aanzetten om actie te ondernemen.

door Carol Woodbury



Bedreiging 10 – Wetten en regelgeving

Wet- en regelgeving? Zijn die niet juist bedoeld om u te helpen met data security? In theorie ja, maar de praktijk is dat de wetgeving ertoe heeft geleid dat de focus niet ligt op de beveiligde oplossing maar op de uitvoerbaarheid van de wet. Neem bijvoorbeeld de mededelingswetten die in Californië en andere staten in de Verenigde Staten zijn aangenomen. Die stellen dat als de gegevens zijn versleuteld – en dat is wat de wet eist – dan is het zelfs niet meer nodig om de getroffenen te informeren als hun gegevens gestolen zijn. Immers, de gegevens zijn versleuteld en ze zijn daarmee veilig. Op het eerste gezicht klopt dat. Maar als we het een en ander wat dieper beschouwen, dan kan het zo zijn dat de gegevens met de gebruikte encryptie helemaal niet veilig zijn gemaakt. De wet zegt niets over het soort encryptie dat gebruikt moet worden, noch over hoe de encryptiesleutel beheerd en beveiligd moet zijn. Een zwakke of 'home-grown' encryptietechniek, en daarbij een slecht ingevoerd sleutelbeheersstructuur, kan ertoe leiden dat gegevens gemakkelijk gedecrypt en dus misbruikt zouden kunnen worden. Wij weten nu allemaal dat er een sterk encryptiealgoritme als AES (256-bit) of 3DES gebruikt moet worden, bij voorkeur in combinatie met het gebruik van PKI-certificaten of wachtzinnen in plaats van wachtwoorden om de gegevens in voldoende mate te beveiligen. Naast het gebruik van encryptie moet er ook de nodige aandacht worden besteed aan het beleid ten aanzien van data security. Alleen dan kan gegarandeerd worden dat de gegevens veilig zijn opgeslagen en bij datatransfer veilig worden uitgewisseld.

Bedreiging 9 – De focus ligt op de controle en veel minder op een veilige implementatie

Bedreiging 10 volgt eigenlijk direct uit bedreiging 9. Sommige beheerders zijn zo sterk gericht op het met goed gevolg afleggen van diverse audits dat zij de implementatie van hun veiligheidsconfiguratie verwaarlozen of er niet of nauwelijks naar omkijken. Ik heb systeembeheerders gezien die applicaties van derden draaien waarbij de security-regels van gebruikers gebaseerd waren op een algemeen gedefinieerde profielen.

Zo'n profiel geeft – zoals de meesten onder u zich al bewust zijn – alle gebruikers die voldoen aan dat profiel het eigenaarschap van alle applicatieobjecten – inclusief gegevensbestanden. Bovendien is de *PUBLIC-autorisatie op de systeem default op *CHANGE gezet. In een geval bevatten deze gegevensbestanden financiële informatie, waardoor het risico voor de privacy en integriteit van de gegevens aanzienlijk was. De beheerder besloot om op deze kwetsbaarheid van het systeem geen actie te ondernemen, omdat de verkoper van de derde partij hen ervan verzekerd had dat hun security solide was (refererend aan hun menugebaseerde security-structuur) en dat zij een SAS70-audit met goed gevolg hadden doorstaan (een SAS70-audit geeft overigens geen regels voor security-procedures). De SAS70-verklaring was voor de interne accountant van deze organisatie voldoende, waardoor er geen opmerkingen op de accountantsverklaring zijn gezet. Aangezien de audit goed was verlopen, koos de beheerder er bewust voor om verder niets te doen aan de kwetsbaarheden van hun systeem – ook al werd dit zeer gedetailleerd uitgelegd. Ik vond dit ontstellend en verontrustend. Ik kan slechts hopen dat de beheerders van de systemen waarop mijn financiële gegevens staan voor een andere benadering kiezen.

> Een geslaagde audit betekent niet noodzakelijkerwijs dat uw systeem en gegevens secure zijn.

De boodschap die deze bedreiging u meegeeft? Een geslaagde audit betekent niet noodzakelijkerwijs dat uw systeem en gegevens secure zijn.

Bedreiging 8 – Conservatisme

Helaas geloof ik dat vele kwetsbaarheden omtrent security onopgelost blijven omdat veel beheerders en programmeurs te conservatief zijn. Ik heb beheerders behoorlijk defensief zien worden als zij gevraagd werden om de kwetsbaarheden in de veiligheid van hun systeem aan te pakken. Deze defensieve houding leidt er vaak toe dat men weigert actie te ondernemen. Het is alsof ze er bang voor zijn om nu actie te ondernemen, waardoor ze dan ontslagen zouden kunnen worden omdat ze geen actie hebben ondernomen in het verleden. Nou, dit is mijn mening over deze kwestie.

Terug in de tijd, toen veel beheerders werden opgeleid, bevonden we ons in de dagen van het groene scherm op de AS/400. Toen waren terminals nog direct aangesloten op het systeem. In die tijd was het vrij gemakkelijk om het systeem te beveiligen. Het enige wat in principe gedaan moest worden, was het configureren van de gebruikers tot gebruikers met beperkte bevoegdheden en de menubeveiliging van de applicatie te gebruiken om hen binnen de juiste menuopties te zetten. Beheerders hoefden geen veiligheidsexperts te zijn en ook hoefden zij niet veel tijd te besteden aan het denken over security. Gelukkig (of helaas, afhankelijk van hoe u het bekijkt), werd het systeem steeds opener en tegelijkertijd complex en was de beveiliging opeens niet meer zo gemakkelijk. Naast deze beveiligingscomplicaties werd het systeem in het algemeen ook complexer om te beheren, en beheerders dienden nog meer taken te vervullen – prestaties, beschikbaarheid, berichtenbeheer, werkroostering, etc. Terwijl het eigenlijk belangrijker was, werd security zelden of nooit als prioriteit benoemd. Nu, door diverse wetten en regelingen en de alsmaar groeiende dreiging van inbreuken, is security eindelijk een prioriteit. De meeste beheerders verwelkomen alle hulp die zij ontvangen en die hun efficiënter maakt en beter op de hoogte brengt van security.
Zij realiseren zich dat hun systeem kwetsbaarheden kent en zoeken naar manieren om deze op te lossen voordat ze een probleem worden. Sommige beheerders weigeren echter te helpen en zeggen dat zij ontslagen zullen worden als zij hun bazen over de kwetsbaarheden informeren. Als ik echter manager zou zijn, zou ik er zeker voor kiezen om over de problemen te spreken voordat zij punt van discussie worden. Ik zou behoorlijk geïrriteerd raken als ik een vraagstuk zou moeten oplossen dat voorkomen had kunnen worden als iemand me erover geïnformeerd had. Ik realiseer me dat er onredelijke bazen bestaan in deze wereld, maar als u een van die beheerders bent die weigeren toe te geven dat er kwetsbaarheden in uw systeem zitten, dan moedig ik u aan om te denken aan de acties die het management vrijwel zeker zal ondernemen mocht zich een inbreuk voordoen op uw systeem waarvan zij dachten dat u deze beveiligd had, en om een proactieve benadering van beveiliging toe te passen. Het afstappen van de defensieve houding kan ook het laten varen van een stukje trots betekenen. Ik realiseer me dat het voor sommige beheerders niet gemakkelijk is om toe te geven dat er problemen bestaan op hun systeem, maar dit is een geval waar hoogmoed en een defensieve houding daadwerkelijk voor de val zouden kunnen komen.

Bedreiging 7 – Nieuwe technologieën

Ik vind dat het meest beangstigende van nieuwe technologieën is dat zij nog niet volledig bewezen zijn, hun echte risico's nog onbekend zijn en het daarom moeilijk is om te weten hoe het risico waar ze verband mee houden, geëlimineerd of op zijn minst beperkt kan worden. Neem RFID (Radio Frequency Identification)-technologie. Op het eerste gezicht lijkt deze technologie onschuldig. Maar wanneer deze embedded in paspoorten zijn opgenomen, dan is het een beetje beangstigend. Er wordt verondersteld dat de regering van de VS stappen onderneemt om uw privacyaspecten van deze nieuwe technologie te waarborgen. Eerlijk gezegd ben ik een beetje sceptisch en vraag me af of ze op de hoogte zijn van de volledige impact van deze nieuwe technologie op onze privacy..

Een andere issue met nieuwe technologieën is dat hun risico ervoor kan zorgen dat zij op mijn lijst als mijn #1 bedreiging of mijn #10 bedreiging terechtkomen – maar ik weet pas welke plaats ze zullen innemen totdat de technologie volwassen is geworden.

De boodschap die deze bedreiging u meegeeft? Laat omwille van de security een technologie rijpen voordat u er aan mee gaat doen. Wees er zeker van dat u zich op uw gemak voelt en de technologie goed genoeg begrijpt om de risico's die eraan verbonden zijn te kennen en, indien nodig, deze te kunnen beperken.

Bedreiging 6 – Gebrek aan opleiding en asociaal gedrag

Deze twee bedreigingen gaan hand in hand, dus heb ik besloten ze te combineren.
Als technische professionals kunnen we >>

vergeten dat de meerderheid van computergebruikers onwetend blijven ten aanzien van de bedreigingen door virussen, phishing en spyware. Ik vind dat het onze plicht is om de mensen om ons heen kennis bij te brengen – of het nu de eindgebruikers op onze werkplek zijn of onze vrienden en familie. Ik werd hieraan herinnerd toen ik tijdens de Thanksgiving-vakantie bij mijn nichtje op bezoek was. Zij toonde mij haar laptop toen er een bericht binnenkwam dat de proefperiode van haar gratis antivirus op punt van verstrijken stond. Ik zei: "Je gaat je antivirus zeker verlengen, toch?" Toen ze schoorvoetend antwoordde "Denk het wel," vertelde ik haar onmiddellijk dat niet verlengen geen optie was en dat ik de verlenging zou betalen als dat het probleem was! Nou wist ze misschien dat een slap antwoord haar Tante Carol tot het betalen van het abonnement zou brengen, maar ik geloof dat de reden voor haar vage antwoord een gevolg was van een gebrek aan kennis. Dus ging ik verder met haar te informeren over het belang van dit soort software en hebben we samen de verlenging van haar abonnement geregeld (en ja, ik heb het betaald). Mijn nichtje is studente verpleegkunde – zeker niet dom – maar je kunt haar ook zeker niet technisch belezen noemen. Toen ik terugkeek op de situatie realiseerde ik me dat ik omgeven ben door veel mensen die – net als mijn nichtje – wat scholing zouden kunnen gebruiken omtrent de gevaren van virussen, phishing (momenteel de populairste vorm van asociaal gedrag – het verkrijgen van informatie door het aannemen van een valse hoedanigheid) en spyware.

De enige reden waarom virussen, spyware en met name phishing succesvol zijn, is omdat mensen onvoldoende op de hoogte zijn. Ze openen bijlagen of beantwoorden een 'officiële mededeling' van een bank of Amazon.com of PayPal eigenlijk alleen maar omdat zij niet weten dat ze dit niet moeten doen. Echter, niemand heeft hun ooit verteld heeft dat het gevaarlijk is om dat te doen. Ze zijn niet technisch, dus lezen ze niet alle waarschuwingen over alle gevaren zoals wij dat doen. Wie kan hen beter hierover informeren dan wij? Ik moedig u aan deze bedreiging te verminderen – breng uw kennis over op uw vrienden, familie en collega's. U zou zelfs kunnen overwegen om een antivirus of antispyware abonnement cadeau te doen voor de volgende verjaardag of tijdens de Kerst voor die vriend of dat familielid waar u altijd moeilijk een cadeau voor vindt!

Bedreiging 5 – Onbeveiligde ontwikkelingssystemen

De meeste organisaties begrijpen de noodzaak van het beveiligen van hun productiesystemen. Wat zij echter vaak niet onderkennen, is dat de noodzaak om hun ontwikkelingssysteem als een productiesysteem te behandelen, en dus met evenveel zorg te beveiligen. Waarom is dit nodig? Want het komt zelden voor dat ontwikkelingssystemen geen productiegegevens bevatten. Ontwikkelaars hebben gegevens nodig om applicaties te testen en met welke gegevens kan beter getest worden dan met echte gegevens? Terwijl dit niet zo'n probleem hoeft te zijn als het om voorraadbeheergegevens gaat, is dit toch zeker wel een belangrijke kwestie als het gegevens betreft over personeel, loonlijsten of creditcards. Waarom is dit een probleem? Omdat ontwikkelaars nu eenmaal meer toegang hebben tot, en vaak meer bevoegdheden op een ontwikkelingssysteem hebben dan op een productiesysteem. Zij hebben daardoor vaak toegang tot zeer gevoelige gegevens. Dit vormt een gevaar, omdat zij over de kennis beschikken van waar de gevoelige gegevens zich bevinden, en in staat zijn de gegevens te verkrijgen zonder dat ze in het systeem opgespoord kunnen worden als het systeem niet op de juiste wijze beveiligd is, of als de ontwikkelaar teveel bevoegdheden heeft en zelf de beveiliging en audit-configuratie zelf kan wijzigen.

De oplossing voor deze bedreiging is het beveiligen van de ontwikkelingssystemen en het verminderen van de bevoegdheden van de ontwikkelaars. Met andere woorden: behandel het ontwikkelingssysteem als een productiesysteem. Een andere mogelijkheid die ik adviseer, is het 'neutraliseren' van gegevens van het ontwikkelsysteem zodat het geen 'echte' gegevens meer zijn en ze behalve voor het testen van de applicatie waardeloos zijn.

Bedreiging 4 – Volledige afhankelijkheid van exit-programma's voor het beveiligen van uw data

Voor degenen onder u die denken dat uw systeem en data goed zijn beveiligd omdat u exit-programma's heeft, is het uitermate interessant kennis te nemen van deze bedreiging. Realiseert u zich dat er geen 'exit-points' zijn voor alle ingangen op het systeem – zoals bijvoorbeeld sockets en een web (http)-applicatie? En heeft u wel eens bedacht dat een exitprogramma niet zal worden aangeroepen als een gebruiker zich toegang verschaft tot data komende van een commandoregel? Maar, zo wordt over het algemeen gedacht, de meeste gebruikers zijn gebruikers met beperkte rechten. Dat begrijp ik, maar het is kenmerkend voor de gebruikers met de meeste kennis van uw systeem en kennis van wat te doen met de gegevens, dat zij toegang tot de commandoregel hebben. Met andere woorden, exitprogramma's zullen u niet beschermen tegen oneigenlijke datatoegang door gebruikers (zoals DBA's, systeemanalisten, ondersteunend personeel, programmeurs, etc.) die een legitieme zakelijke behoefte hebben aan toegang tot de commandoregel.

Ik zeg niet dat u uw exit-point-software weg moet gooien – maar wees u bewust van het juiste gebruik ervan. Als u het netwerkverkeer (FTP, OBDC, etc.) van uw systeem moet loggen of monitoren, of ervoor moet zorgen dat er een alarmsignaal wordt afgegeven als iemand een bepaald bestand probeert te downloaden, dan zijn exit-programma's de enige manier om dat te doen. Of als u een persoon toestaat om ODBC te gebruiken in plaats van FTP, dan kunnen exit-points worden aangeroepen. Of, als u ten aanzien van multiple layer een defensieve toegangsstrategie heeft, dan zijn exit-programma's zeker het overwegen van het toevoegen waard.

Als u echter exit-programma's gebruikt als uw enige middel van toegangscontrole tot bestanden met gevoelige gegevens, dan moedig

U zou zelfs kunnen overwegen om een antivirus of anti-spyware abonnement cadeau te doen voor de volgende verjaardag of tijdens de Kerst voor die vriend of dat familielid waar u altijd moeilijk een cadeau voor vindt!

ik u aan die strategie te heroverwegen. Wat me bij de volgende bedreiging brengt…

Bedreiging 3 – Gebrek aan gebruik van i5/OS- en OS/400-objectbeveiliging

Beveiliging op objectniveau bestaat al sinds de introductie van de System/38. De meeste beheerders en leveranciers negeerden deze geïntegreerde feature van het besturingssysteem omdat het zo gemakkelijk was om het systeem te beveiligen (zie bedreiging 8). Daarom bevinden we ons vandaag de dag in de situatie waarbij er op de meeste systemen geen gebruik wordt gemaakt van deze sterke feature. Beveiliging op objectniveau is de enige methode voor toegangscontrole die altijd aanwezig is – om het even hoe toegang wordt verkregen tot een object (bijv. een gegevensbestand) – via een commandoregel, socketprogramma, internetapplicatie, FTP, JDBC, etc. Ik ben het dus oneens met degenen die beweren dat beveiliging op objectniveau te lastig is om te implementeren, of dat het geïmplementeerd moet worden voor elk object op het systeem. Geen van beide beweringen is waar. Er kan een substantiële beveiliging worden gerealiseerd door het beveiligen van de bibliotheken van de applicaties die gevoelige gegevens bevatten. Neem bijvoorbeeld uw applicatie voor loonkosten/staten (Payroll). Wie zouden toegang moeten hebben tot de gegevens van deze applicatie? Het gaat dan om gebruikers in Payroll- en mogelijkerwijs Personeelsprogramma's en applicaties voor het bijhouden van werkuren, correct? Dus stel *PUBLIC-autorisatie in op *EXCLUDE en ken dan de Personeels- en Payroll-groep evenals de tijdregistratieapplicatie het profiel *USE toe aan de Loonadministratie en dan heeft u een uitermate gevoelige applicatie gesloten voor de meerderheid van uw gebruikers. Ja, u kunt het ook naar het volgende niveau brengen en uiteraard de objecten in de payroll libraries beveiligen. Maar dat is niet nodig als u voor het eerst aan de gang gaat met de security op objectniveau. U kunt gemakkelijk aan de slag gaan met dat gedetailleerde niveau als u er zeker van bent dat de security op objectniveau van de bibliotheek naar behoren functioneert.

Bovendien vereist een groot aantal van de huidige wetten en regels exclusieve toegangscontrole. Met andere woorden: het gebruik van beveiliging op objectniveau. Bijvoorbeeld de Data Security Standards van de Betaalkaartenindustrie (PCI – Payment Card Industry) vereisen op exclusiviteit gebaseerde toegang. Dat wil zeggen dat >>

Waarom vind ik een geschreven en goedgekeurd security-beleid zo belangrijk? Omdat het een bewijs is van het belang dat uw organisatie stelt in security.

de toegangscontroles op bestanden die informatie over creditcards bevatten, zodanig moeten worden geconfigureerd dat alleen gebruikers met een directe zakelijk link toegang wordt gegeven tot het bestand. Vertaald naar i5/OS-termen betekent dit dat het niet volstaat om enkel te vertrouwen op de 'menubeveiliging' van een applicatie waar het de toegangscontrole betreft. De beveiligingsstructuur van de applicatie met bestanden met creditcardinformatie moet worden ingesteld op *PUBLIC *EXCLUDE en alleen gebruikers die toestemming hebben

gekregen voor toegang tot het bestand buiten het bereik van de applicatie (zoals via ODBC), moeten extra autorisaties verkrijgen.

Bedreiging 2 – Geen security-beleid

Waarom vind ik een geschreven en goedgekeurd security-beleid zo belangrijk? Omdat het een bewijs is van het belang dat uw organisatie stelt in security. Het is ook een bewijs van het feit dat de organisatie haar behoeften heeft onderzocht en haar security-beleid en strategie heeft bepaald. Het niet hebben van zo'n beleid is een bedreiging, omdat het een gebrek aan betrokkenheid en begrip aangeeft van de zijde van het management. Het management vindt security geen essentiële zaak – en security wordt een eenmalig IT-project dat voltooid is en nooit meer aan de orde komt. Een solide security-beleid is de fundering om zeker te zijn van betrokkenheid en toewijding aangaande dit onderwerp. Daar komt bij dat het security-beleid uiteraard juridische aspecten heeft. Wat is de betrokkenheid van de organisatie ten aanzien van de security en wat zijn de gehanteerde procedures. Tenslotte kan men slechts gissen naar het oordeel van een rechtbank als zich een inbreuk voordoet. Het gedaagde bedrijf zal gevraagd kunnen worden naar een formeel passend security-beleid.

Wat me bij de belangrijkste bedreiging van vandaag brengt…

Bedreiging 1 – Apathie

Ik vind het ongelooflijk beangstigend als ik iemand tegenkom die het gewoonweg niet uitmaakt dat er niet-beveiligde onderdelen op hun systeem of netwerk zitten, of dat ze geen strategie voor virusscannen of directe programmawijziging voor hun PC's hebben. Zij nemen de houding aan van 'het is tot nu toe niet voorgekomen, dus waarom zou ik iets moeten doen aan mijn security'.
Mijn reactie op die houding is ten eerste: omdat u geen aandacht besteedt aan uw security-configuratie, hoe kunt er dan zo zeker van zijn dat er (nog) niets is gebeurd? Ten tweede: hoe garandeert een 'event '-vrij verleden een 'event'-vrije toekomst? Nieuwe technologieën brengen gegevens in de openbaarheid waar dat tot voor kort niet het geval was. Verder worden er dagelijks nieuwe virussen en spyware verspreid, verandert de houding van werknemers, worden er nieuwe werknemers aangenomen die beschikken over grote technische vaardigheden, en worden er per ongeluk applicaties geschrapt omdat iemand eigenlijk over teveel autorisaties beschikt. Ik stel mij daarom steeds dezelfde vraag: hoe garandeert een 'event'-vrij verleden een 'event'-vrije toekomst?

Ik begrijp apathie niet omdat ik van nature proactief ben. Ik denk dat apathie onze belangrijkste bedreiging is omdat het te maken heeft met attitude of houding. De houding van de beheerder bij mijn bank of verzekeringsmaatschappij, of de houding van een medewerker bij het clearing house dat mijn creditcardtransacties verwerkt. "Maar," zegt u, "er zijn wetten en regels die deze gegevens beschermen." Dat is waar. Maar de houding van apathie leidt er in praktijk toe dat deze mensen wetten en regels negeren. En dat omdat ze denken dat ze niet gepakt zullen worden en dat er geen audits zullen plaatsvinden. Dat alles maakt dat mijn gegevens onbeveiligd zijn. Ik heb die houding meegemaakt. Die houding bestaat ook in de i5/OS-wereld. En zolang die bestaat, zullen mijn gegevens – en de uwe – openbaar kunnen komen. •

Carol Woodbury is medeoprichter van SkyView Partners, Inc., een bedrijf dat gespecialiseerd is in 'security compliance management', evaluatiesoftware en beveiligingsdiensten. Carol is voormalig AS/400-beveiligingsarchitect voor IBM in Rochester, Minnesota, en heeft zich gedurende meer dan 15 jaar gespecialiseerd in beveiligingsarchitectuur, design en consultancy. Carol houdt tevens over de hele wereld keynote speeches over uiteenlopende veiligheidsonderwerpen en is medeauteur van het boek 'Experts' Guide to OS/400 and i5/OS Security'.

De System i-producten van SkyView Partners – SkyView Risk Assessor en SkyView Policy Minder – worden via Halcyon Software in de Benelux op de markt gebracht door SRC Secure Solutions BV (www.srcsecuresolutions.eu). Met SkyView Risk Assessor worden security-bedreigingen op de i5 opgespoord, waarover in een uitgebreide detailanalyse wordt gerapporteerd. In SkyView Policy Minder wordt het security-beleid van een bedrijf vastgelegd en vervolgens continu bewaakt. Het pakket zorgt er eveneens voor dat eventuele aanpassingen daarin worden gesignaleerd en aan de verantwoordelijke, zoals de Security Officer, worden gemeld. Uiteraard worden aanpassingen in het security-beleid van een bedrijf direct via de Policy Minder opgenomen en verwerkt.