De bedreigingsomgeving:

BEVEILIGINGSUITDAGINGEN EN INNOVATIE VAN FINANCIËLE DIENSTVERLENING

De slechte reputatie van internet op het gebied van beveiliging belemmert de brede acceptatie van financiële online diensten. Dit is gedeeltelijk het gevolg van het feit dat bij de ontwikkeling van deze diensten systematisch te weinig aandacht wordt besteed aan beveiligingseisen, wat resulteert in meer online fraude en beveiligingsincidenten dan nodig is. De financiële dienstverleningsindustrie moet met betrekking tot de ontwikkeling van nieuwe producten haar benadering op dit gebied verbeteren, wil zij het vertrouwen van de consument in het online aanbod winnen. Alec Shuldiner bespreekt het product-ontwikkelingsproces en biedt suggesties voor een systematische verbetering hiervan.

PHD. ALEC SHULDINER, BASEL CONSULTING

De financiële dienstverleningsindustrie profiteert misschien meer dan enige andere industrie, van de voortdurende groei van internet. De meeste van haar activiteiten zijn reeds gedigitaliseerd, zodat meer producten geschikt zijn voor online marketing en distributie. En uiteindelijk belooft internet een veel effectievere beveiliging voor alle soorten financiële transacties.

Dit laatste punt is er één dat door velen zal worden betwist: internet wordt doorgaans meer gezien als speelplaats voor fraudeurs en hackers, dan als een uiterst veilig netwerk. Maar naarmate oplossingen voor encryptie, identificatie en verificatie steeds beter worden, zal de reputatie van internet zich op gelijke wijze ontwikkelen vanuit haar huidige 'Wild West'-imago; uiteindelijk zal het misschien zelfs door zowel financiële instellingen als de consument als veiliger worden beschouwd dan offline transacties, of zelfs via gesloten netwerk.

Intussen echter, zijn er veel tegenslagen geweest en er zullen er nog veel meer volgen. Tot op zekere hoogte zijn deze tegenslagen onvermijdelijk – dit is nog steeds een betrekkelijk nieuw en complexer wordende technologie – maar het grote aantal fraude- en beveiligingsincidenten dat zich tot nu toe heeft voorgedaan, is veel hoger dan noodzakelijk. De algemene perceptie van internetveiligheid is als gevolg daarvan veel negatiever dan nodig is. Dit is geen onbelangrijke kwestie: de slechte reputatie van internet wat betreft beveiliging heeft een aanzienlijk vertragend effect op de acceptatie van financiële online diensten op consumenten en vormt de oorzaak van het mislukken van veel projecten die anders misschien zouden zijn geslaagd.

Waarom zijn er onvoldoende veilige financiële sites opengesteld voor het publiek? Gedeeltelijk omdat de lancering van dit soort nieuwe producten niet voldoende aandacht heeft gekregen van verantwoordelijke bankautoriteiten (hoewel dit begint te veranderen) of van andere verantwoordelijke autoriteiten. Gedeeltelijk ook omdat veel van de basissoftware die wordt gebruikt voor het leveren van deze producten (zoals bedieningssystemen voor firewalls en servers) ongedocumenteerde kwetsbaarheden bevat. Maar de belangrijkste reden is dat in het huidige proces van internet-innovatie binnen de meeste financiële dienstverleningsbedrijven – zowel startende als gevestigde ondernemingen – niet voldoende middelen worden besteed aan beveiliging tot het moment dat een nieuw product zichzelf functioneel en commercieel heeft bewezen. Om te begrijpen waarom dit zo is, en hoe deze structurele zwakheid het beste kan worden aangepakt, moeten we eerst eens nauwkeurig kijken naar het ontwikkelingsproces van het project.

Het beheren van de beveiliging

De ontwikkeling van nieuwe producten gebeurt doorgaans op projectbasis. Dit betekent dat er een functioneel doel wordt vastgesteld en een beperkte hoeveelheid ontwikkelingstijd, financiering en personeel wordt vrijgemaakt om dit doel te verwezenlijken. Dat het uiteindelijke project 'veilig' moet zijn, is vaak vanzelfsprekend of wordt, in het optimale geval, vermeld als één van de eigenschappen aan de hand waarvan het succes van het project uiteindelijk wordt afgemeten. Het komt echter maar zelden voor dat een project begint met een risicoanalyse, zonder welke de ware omvang van het beveiligingsprobleem niet nauwkeurig kan worden bepaald.

Vanuit een beveiligingsperspectief is de eerste stap van het project daarom in de meeste gevallen de verkeerde stap: om optimaal effectief te zijn (en op de meest efficiënte wijze te worden gerealiseerd) dient beveiliging van het begin af aan te worden ingebouwd in het projectontwerp. Als dit niet wordt gedaan, zal er naar alle waarschijnlijkheid een aantal dingen gebeuren:

• Het productconcept wordt ontwikkeld zonder rekening te houden met beperkingen of extra functionaliteit, die later door beveiligingseisen

Definitie van risicoanalyse

'Risicoanalyse': Een document waarin de operationele en technische risico's worden beschreven die van toepassing zijn op een bepaald product of een bepaalde activiteit.
Het dient:
• de verschillende operationele en technische probleemgebieden volledig te definiëren (b.v. 'toegangscontrole' of 'bedrijfscontinuïteitsbeheer');
• voor elk van deze gebieden de betreffende risico's te vermelden en onder te verdelen in ten minste twee categorieën: beheerste risico's (dat wil zeggen risico's die geminimaliseerd of afgedekt zijn) en geaccepteerde risico's. Een goede risicoanalyse definieert niet alleen de betreffende risico's, maar wijst ook verantwoordelijkheid aan voor de beheersing of acceptatie van elk hiervan.

zouden kunnen worden opgelegd. Wanneer het productconcept eenmaal definitief is bepaald, wordt het veel moeilijker (en ook nog eens een stuk duurder) het aan te passen aan deze beperkingen of er functionaliteit aan toe te voegen.

• Het technisch ontwerp, inclusief softwareselectie of -ontwikkeling, netwerk-architectuur, communicatieregelingen en hardwareselectie, zal worden ontwikkeld met een lappendeken aan beveiligingsmaatregelen, die elk naar de willekeur van de verschillende ontwerpers of leveranciers worden toegevoegd, in plaats van een allesomvattend en daardoor effectiever beveiligingsontwerp. Dit kan een latere risicoanalyse gecompliceerder maken (en zal daardoor waarschijnlijk ook een minder nauwkeurige weergave vormen van de werkelijke risico's) en kan zelfs tegenstrijdige beveiligingselementen introduceren in het product.

• Externe partners kunnen worden gekozen zonder voldoende aandacht te schenken aan hun vermogen een veilige oplossing te kunnen leveren, of een oplossing die goed kan worden geïntegreerd met de beveiligingselementen van andere onderdelen van het project.

• Beveiligingsbewustzijn onder projectmedewerkers zal lager zijn dan noodzakelijk, met als gevolg dat informatie over de technologie te vrij wordt verspreid, waardoor het veel eenvoudiger wordt voor kwaadwillenden de informatie te vinden die zij nodig hebben om op een later tijdstip aanvallen uit te voeren op het systeem.

Omdat het project primair zal worden beoordeeld op wat het kan doen en niet op wat het kan voorkomen, zal het compromis tussen functionaliteit en beveiliging vrijwel altijd in het voordeel uitvallen van functionaliteit. En bij de meeste projecten komen veel van dit soort compromissen voor.

De testfase

Als de meeste projecten niet beginnen met beveiligingskwesties, op welk punt wordt de beveiliging dan meestal beoordeeld? Alleen een echt onverantwoordelijk (of wanhopig) bedrijf introduceert een product online zonder het uitvoeren van een dergelijke evaluatie. Bij de meeste projecten doen zich inderdaad tijdens de ontwikkeling beveiligingsproblemen voor, hoewel deze slechts stukje bij beetje worden aangepakt. Maar bij het doorsnee project zal beveiliging doorgaans pas uitgebreid worden aangepakt als het moment is aangebroken om de testfase te beginnen.

Hoe een systeem zich onder operationele omstandigheden zal gedragen, kan onmogelijk met volledige zekerheid worden voorspeld. Dit geldt vooral voor de complexe systemen die gewoonlijk vereist zijn voor het leveren van financiële producten. Om de geschiktheid van een systeem te beoordelen voor een commerciële introductie, wordt het daarom doorgaans onderworpen aan een aantal tests die moeten aantonen hoe het gehele systeem werkt. Om een goede indicatie te geven van hoe het systeem zal functioneren wanneer het via internet wordt aangeboden, moeten deze tests worden uitgevoerd op een netwerk en bij voorkeur een netwerk dat een nauwkeurige afspiegeling is van de daadwerkelijke productieomgeving die zal worden gebruikt om het commerciële systeem te bedienen. Het maken van de overstap van een systeem dat bestaat binnen de pc's van ontwikkelaars op een systeem dat daadwerkelijk op een netwerk loopt, is een enorme stap in de richting van de commerciële toepassing. Het is in deze stap dat de aandacht zich doorgaans concentreert op beveiligingskwesties en als (!) er een algemene evaluatie moet plaatsvinden vóór de commerciële introductie, dan zal deze naar alle waarschijnlijkheid op dit punt plaatsvinden.

Beveilingsuitgaven, weggegooid geld?

Dat is veel te laat. Na wat waarschijnlijk een aanzienlijke dosis inspanning en behoorlijk wat tijd heeft gekost, heeft het gehele team – marketing, it, operations, de mogelijke externe partners en niet te vergeten de interne supervisiecommissies en het hoger management – bereikt wat de meeste mensen waarschijnlijk zien als de laatste stap vóór de commerciële introductie. De druk is hoog en tijd is op dit moment uiterst kostbaar. Een beveiligingsinspectie zal waarschijnlijk zeer snel moeten worden uitgevoerd en als die inspectie in deze fase grote problemen aan het licht brengt, staat de projectmanager voor een enorm moeilijke beslissing. Een grote wijziging zou een gevaar kunnen vormen

voor het project zelf, en zal in ieder geval de vaart en het moreel aantasten. Zelfs kleine punten zullen waarschijnlijk alleen worden aangepakt als de commerciële introductie toch al wordt uitgesteld in verband met andere technische of marketing- wijzigingen. In de meeste van dit soort gevallen verschijnt beveiliging laat ten tonele waarna deze er snel weer vanaf wordt gehaald.

De bedreigingsomgeving

Dat de ontwikkeling van een nieuwe product in veel gevallen op deze manier mag doorgaan, is logisch in het licht van de huidige houding van de financiële branche. Het is per slot van rekening moeilijk te raden welke schaarse projecten zullen slagen en voor de vele projecten die dat niet doen, zullen de beveiligingsuitgaven eenvoudig weggegooid geld blijken. Anderzijds mogen succesvolle projecten zich onveilig ontwikkelen omdat men denkt dat de extra onkosten van het corrigeren ervan, wanneer hun waarde eenmaal is aangetoond, in totaal goedkoper is dan de kosten van het uitvoeren van de beveiliging van de grond af aan, vlak voor alle projecten, zowel succesvolle als mislukte.

Dit kan waar zijn, maar net zo goed niet. Voor de meeste ondernemingen in deze sector is dit een ongetoetste aanname.

Onderzoek naar de kosten rond de ontwikkeling van een nieuw product zou kunnen aantonen dat de wijzigingen die in of zelfs na de testfase nodig bleken om te kunnen voldoen aan beveiligingseisen inderdaad hoger zijn dan de gecombineerde kosten van beveiligingsmaatregelen van de grond af aan voor alle projecten, succesvol of niet. Men kan zich ook afvragen hoeveel projecten mislukken als gevolg van verlammende beveiligingszwakheden die vóór of na de introductie worden ontdekt. In het laatste geval zijn al deze middelen vanzelfsprekend verspild.

Nog erger is dat deze benadering voorbijgaat aan één belangrijk feit: internet is, zoals het Wilde Westen in de dagen van de Amerikaanse kolonisten, een bedreigingsomgeving en in sommige opzichten zelfs een nog onveiliger omgeving dan die in dat wetteloze tijdperk. De banken die door de bandieten werden overvallen bevatten slechts een beperkte hoeveelheid geld, en verhalen over de tegenspoed van een beroofde bank reikten niet ver. Op internet is geen van beide waar: de schade die kan worden veroorzaakt door een serieuze hacker is grenzeloos en de afstand die het slechte nieuws kan afleggen onbeperkt. Eén groot incident kan je beneden het aanvaardbare gemiddelde doen zakken.

Het verbeteren van projecten

Het ontwikkelingsproces van nieuwe producten moet worden verbeterd als de financiële dienstverleningssector haar naam en reputatie online wil verbeteren. Een paar suggesties:

- *Betaal op voorhand voor beveiliging*: ontwikkel middelen om nauwkeurig de beveiligingskosten van voorgestelde projecten in te schatten; vergeet niet de vereisten voor de juiste scheiding van functies bij het inschatten van het aantal mensen dat voor het project vereist is.
- *Herconstrueer interne beveiligingsmiddelen zodat zij beter voldoen aan de behoeften van opstartprojecten:* eis dat alle betreffende projecten gebruikmaken van geherconstrueerde interne beveiligingsmiddelen; verwerk deze interne kosten in de kostenramingen voor het project.
- *Maak beveiliging tot een beoordelingscriterium voor projectmanagers:* biedt projectmanagers een beveiligingstraining aan.
- *Stel de risico's vroeg vast*: eis risicoanalyses voor ieder project voordat er een projectplan wordt ontwikkeld voor de testfase.
- *Bereid je voor op een ramp:* stel een rampenplan op zodra de pers verslag begint te geven over een bepaald project.
- *Kweek een beveiligingsmentaliteit:* zorg ervoor dat de ontwikkeling van nieuwe producten een hoge beveiligingsclassificatie krijgen, zelfs als deze zich nog in de brainstormfase bevinden.
- *Kies geen kwetsbare partners:* werk niet samen met externe partners die geen risicoanalyses kunnen geven van hun eigen relevante activiteiten of niet voldoende documentatie kunnen verstrekken van hun capaciteiten en procedures.
- *Zeg het voort*: Grote financiële instellingen dienen in een vroeg stadium belangen te nemen in beginnende financiële ondernemingen en deze belangen te gebruiken voor het geleidelijk inprenten van beveiliging als een waarde: iedere onveilige online dienst, of die nu wordt aan geboden door een klein startend bedrijf of door een gevestigde financiële instelling, kan de publieke perceptie ondermijnen van alle online diensten.

Financiële instellingen zullen nieuwe online diensten blijven aanbieden; dat is zo goed als onvermijdelijk, gegeven de potentiële kostenbesparingen en de nieuwe mogelijkheden die deze omgeving biedt. Maar kostenbesparingen zijn voor de eindgebruiker van weinig belang, en zelfs de verleiding van nieuwigheidjes zal worden genegeerd als dit de opoffering inhoudt van de gemoedsrust die op dit moment in verband wordt gebracht met dienstverlening op het gebied van bankieren, verzekeren, en de meeste andere financiële zaken. Om dit doel te bereiken zijn langzame maar zekere stappen vereist.•

Phd. Shuldiner is founder and principal consultant at Basel Consulting, a design and management consultancy focused on complex IT projects. Please direct feedback or questions on this article to alec@baselconsulting.com.