Online Security & Hosting

Online Security & Hosting

Een webshop starten is tegenwoordig een fluitje van een cent, maar er komt daarna nog veel meer bij kijken. Met name op het gebied van online security dienen zich uitdagingen en verantwoordelijkheden aan. Voor retailers is het belangrijk om zich bewust te zijn van de risico's en bekwaam om ze te voorkomen of op te lossen.

ShoppingTomorrow/ Online Security & Hosting

1. Wat staat webshops te wachten?

Nederland kent een zeer actieve e-commerce-gemeenschap. Er waren in 2014 naar schatting zo'n 59.000 webshops en dit aantal groeit met de dag. Dankzij de goede IT-infrastructuur is het ook eenvoudig om een webshop te starten. Er zijn hostingbedrijven genoeg die een compleet pakket aanbieden voor nog geen 10 euro per maand.

1.1 Risico's voor webshops

Dat het eenvoudig is om een webshop te starten wil nog niet zeggen dat er over alles is nagedacht. Een webshop-eigenaar moet een hoop regelen, waarbij doorgaans het eerst wordt gedacht aan logistiek en betalen. Een vaak vergeten aspect van het exploiteren van een webshop is het goed inschatten van risico's.

Die risico's kunnen variëren van het platliggen van de shop door storingen, softwareproblemen of digitale aanvallers, hackers en online criminelen. Een webwinkelier die zich goed wil kunnen verdedigen tegen digitale dreigingen moet eerst weten waaraan hij kan worden blootgesteld. De effecten kunnen enorm zijn, tot aan het moeten sluiten van de webshop aan toe. Daarnaast geldt dat er niet alleen wordt gejaagd op de grote vissen zoals onlangs eBay.[1][2] Ook voor de kleine webwinkels loeren hackers op een mooie of makkelijke vangst, waardoor informatiebeveiliging ook voor hen steeds relevanter wordt.[3]


Nieuws

Nagemaakte webshop Computerland verspreidde malware

donderdag 14 augustus 2014, 13:21 door **Redactie**, 6 **reacties**

Oplichters hebben onlangs de webshop van de computerketen Computerland nagebouwd en gebruikt voor het oplichten en infecteren van klanten met malware. De domeinnaam die de oplichters gebruikten, computerland-outlet.nl, werd op 3 augustus via hostingbedrijf Versio geregistreerd.

Artikel over nagemaakte webshop Computerland


Nieuws

PostNL waarschuwt klanten voor besmette e-mails

zaterdag 18 oktober 2014, 08:39 door **Redactie**, 34 **reacties**

PostNL heeft klanten een e-mail gestuurd waarin het waarschuwt voor valse e-mails die op dit moment rondgaan en van het postbedrijf afkomstig lijken, maar in werkelijkheid malware bevatten. Ook op 13 oktober waarschuwde PostNL via **Twitter** dat er valse e-mails in omloop waren, maar de waarschuwing is nu herhaald. Zowel via de website als een e-mail aan klanten. Opmerkelijk is dat PostNL op **Twitter** over "phishing" spreekt, terwijl er helemaal geen sprake van phishing is. Bij phishing wordt geprobeerd om gegevens te stelen, terwijl de besmette e-mails die nu in omloop zijn een heel ander doel hebben.

De valse e-mails stellen dat er een pakket niet kon worden afgeleverd en gebruikers meer informatie via een link in het bericht kunnen vinden. De link wijst echter naar een nagemaakte website van PostNL. Daar moeten gebruikers een captcha invoeren

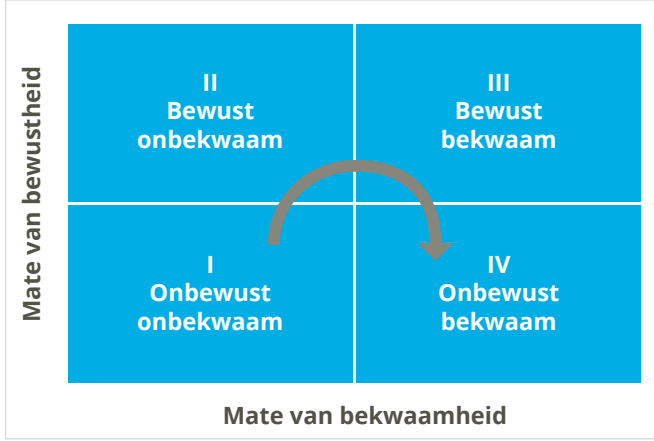
Artikel over waarschuwing PostNL na gemailde malware

REFERENTIES

[1] *Reuters over eBay-waarschuwing 'cyber attack' http://www.reuters.com/article/2014/05/21/us-ebay-password-idUSBREA4K0B420140521*
[2] *Cnet over eBay-waarschuwing voor malware http://www.cnet.com/news/ebay-hacked-requests-all-users-change-passwords/*
[3] *NRC.next: 'Bij best veel winkeltjes kan de hacker jatten' (NRC.next, 2 april 2013) https://www.digisafe.info/Data/digisafe/files/nrc-onderzoek-digisafe.pdf*

Ook maakt een webshop-eigenaar deel uit van de digitale samenleving en beheert hij digitale identiteiten en een schat aan persoonlijk informatie van klanten: zaak dus om hier zeer zorgvuldig mee om te gaan. Wie wil er immers genoodzaakt zijn om melding te maken van het lekken van privacygevoelige informatie?

Heeft u weleens gehoord van SQL-injections, Cross-site scripting, DDoS-aanvallen, brute-force attacks en social engineering? Zo niet, lees dan vooral verder. Zo gaan wij u helpen van onbewust onbekwaam naar bewust bekwaam te komen als het gaat om digitale veiligheid. Wie wel eens van de genoemde ellende heeft gehoord, vindt hier veel informatie om nog beter bestand te zijn tegen digitaal onheil.



Mate van bewustheid en bekwaamheid

1.2 Digitale Dreigingen Model

Om bewust te raken van de bedreigingen waaraan een webshop en haar klanten blootstaan, werken wij met een Digitale Dreigingen Model. Met dit model kunt u zelf heel eenvoudig bepalen welke risico's u loopt en hoe risicovol uw profiel als webshop-eigenaar is. De vragenlijst helpt om vast te stellen welke risico's u loopt.

Wanneer het persoonlijke risicoprofiel is vastgesteld geeft een raamwerk aan welke maatregelen u dient te nemen om digitale dreigingen te verminderen of zelfs helemaal weg te nemen. Dit geeft waardevolle inzichten in passende praktische maatregelen. Geen lange lijsten met complexe modellen, maar een op maat gesneden advies, samengesteld door experts uit het vak.

Van onbewust naar bewust

Aan de hand van de onderstaande vragenlijst worden retailers naar een bepaald risicoprofiel geleid. Op deze manier krijgen zij in korte tijd een indicatie welke risico's relevant zijn. De antwoorden op de vragen zijn gecategoriseerd naar weinig, gemiddelde en grote impact (ofwel: risico). Tevens zijn aan de antwoorden punten toegekend: weinig punten bij een lage impact, veel punten bij een hoge impact. Voor elke antwoord ontvangt u punten (guppy: 1, tonijn: 3, walvis: 5). Na het optellen van de punten, komt u uit bij een bepaald risicoprofiel (guppy is laag, tonijn midden en walvis hoog) met een bijbehorende beschrijving en handreiking van te nemen maatregelen. Let wel: de risicoprofielen zijn indica.

Vraagstelling naar onderwerp	Guppy	Tonijn	Walvis
Privacy			
Hebt u vestigingen buiten Europa?	Nee	Ja, met hoofdkantoor in EU	Ja, met hoofdkantoor buiten EU
Hebt u IT-systemen buiten Europa?	Nee, enkel in Nederland	Nee, enkel in Europa	Ja, enkel buiten Europa
Hoeveel klantgegevens slaat u op?	+5.000	+100.000	+500.000
Welke persoonsgegevens slaat u op?	NAW-gegevens	Financiële data	Data gezondheidszorg
Payment			
Staat u creditcard betalingen toe?	Nee	Nee, enkel iDeal en acceptgiro	Ja, creditcard betalingen
Besteedt u het betalingsverkeer uit (payment service provider)?	Ja, dit is volledig uitbesteed	Gedeeltelijk uitbesteed	Nee, ik regel alles zelf
Hoeveel online bruto omzet genereert u op jaarbasis?	0 tot 100.000 euro	100.000 tot 2 miljoen euro	2+ miljoen euro
Continuïteit			
Welk percentage van uw omzet is afkomstig van online verkopen?	0 tot 30%	30 tot 60%	60 tot 100%
Hoelang kunt u zonder e-commerce-omgeving zonder substantieel omzet te verliezen?	Tot 3 dagen	Tot 1 dag	Tot 1 uur
Hoeveel ICT-leveranciers hebt u voor uw webshop?	1 of 2	3 of 4	4+
Reputatie			
In het geval van een incident (in dit geval website offline), komt u dan in de media?	Nee, daar zal geen aandacht aan besteed worden	Ja, misschien wat berichtjes op internet / lokale kranten	Ja, voorpagina nieuws / NOS journaal
In het geval van een incident (in dit geval foutieve prijzen), komt u dan in de media?	Nee, daar zal geen aandacht aan besteed worden	Ja, misschien wat berichtjes op internet / lokale kranten	Ja, voorpagina nieuws / NOS journaal
In het geval van een incident (in dit geval het uitlekken van klantgegevens), komt u dan in de media?	Nee, daar zal geen aandacht aan besteed worden	Ja, misschien wat berichtjes op internet / lokale kranten	Ja, voorpagina nieuws / NOS journaal
Aantal antwoorden	... 1x = ... punten	... 3 x = ... punten	... 5 x = ... punten
	Totaal aantal punten =		

Vragenlijst voor bepalen van uw risicoprofiel

Van onbekwaam naar bekwaam

De vragen, antwoorden en handreikingen zijn toegespitst op de volgende risicogebieden: privacy, payment, continuïteit en reputatie. Aan de hand van de ingevulde vragenlijst kan een retailer zijn risicoscore te berekenen.

Guppy
13-29 punten. Uw webshop loopt relatief weinig risico. Een korte tijd uitval van uw webshop zal over het algemeen niet leiden tot grote financiële verliezen of grote imagoschade. Uw webshop wordt gezien als een guppy op het grote internet en zal niet direct de aandacht trekken tussen de grote vissen. Hackers zullen niet direct aandacht voor specifiek uw webshop hebben, al valt dit risico nooit uit te sluiten. Hackers scannen namelijk het hele internet af op zoek naar zwakke plekken in security. Zorg er dus voor dat de basics op orde zijn.

Security-maatregelen die u in ieder geval dient te treffen zijn:

- **Privacy:** Als u persoonsgegevens (zoals NAW-gegevens of e-mailadressen) verwerkt, moet u bewerkersovereenkomsten sluiten met uw ICT-toeleveranciers waarin u afspreekt hoe deze toeleveranciers de persoonsgegevens beschermen
- **Payment:** Zorg voor een sluitende financiële administratie waarin de bestellingen van de klanten te relateren zijn aan de betalingen. Dit kan geautomatiseerd worden via goede logging en het regelmatig maken van een uitdraai van deze logbestanden
- **Continuïteit:** Sluit in ieder geval een overeenkomst met de leverancier van uw webshop waarin beschreven staat van welke garanties u uit kunt gaan (denk aan up-time, onderhoudswindows en performance)
- **Imago:** Zorg voor een mogelijkheid om buiten uw webshop om te kunnen communiceren met uw klanten, voor het geval de webshop toch uitvalt of gehackt wordt. Denk aan een Facebook-pagina of Twitter-account (waar u een ingewikkeld wachtwoord kiest dat u goed geheim houdt).

Tonijn
30-47 punten. Uw webshop valt in een gemiddeld risicoprofiel. Dat betekent dat u de nodige aanvullende aandacht aan security moet besteden om te voorkomen dat u financiële of imagoschade oploopt. Hoewel uw webshop gemiddeld gezien geen grote aandacht zal trekken uit de hackerswereld, is de kans groot dat u geregeld last heeft van hackers die 'aan de voordeur rammelen' om eens te zien of u uw zaakjes op orde heeft. Zie uw website als een tonijn in de zee van het grote internet: niet iedereen vindt u interessant, maar er zijn diverse tonijnvissers die het specifiek op u voorzien hebben.

Bovenop de security-maatregelen voor het profiel Guppy, moet u ook denken aan:

- **Privacy:** Het goed beveiligen van persoonsgegevens van uw klanten is belangrijk. Test regelmatig de security van de webshop via security-scans of audits (penetratie-tests). Als u maatwerk-software gebruikt, maak dan afspraken over secure development
- **Payment:** Sluit een contract af met een payment-provider die voor u het betalingsverkeer afhandelt (ga dit niet zelf programmeren). Controleer in het contract welke garanties de provider u geeft en welke plichten u heeft
- **Continuïteit:** Breng uw webshop onder bij een professionele hostingpartij die het volledige beheer van uw totale webshop voor u uitvoert (managed hosting), inclusief de coördinatie met eventuele andere ICT-leveranciers die onderdelen van uw webshop leveren (toeleveranciers)
- **Reputatie:** Tref specifieke maatregelen om reputatieschade via uw webshop tegen te gaan. Controleer content alvorens deze te publiceren (het zogenaamde '4-ogen-principe') en zorg voor technische noodscenario's die gehanteerd kunnen worden bij uitval, hacking, DDoS-aanvallen en dergelijke.

Walvis
48-65 punten. Uw webshop loopt bovengemiddeld veel risico. Uitval van de omgeving of inbraak heeft grote gevolgen voor uw organisatie. Ook is uw webshop belangrijk genoeg voor hackers om te proberen binnen te komen en privacygevoelige gegevens van uw klanten te stelen of te zien of frauduleuze handelingen mogelijk zijn. Publicatie van verstoringen of een hack zal niet onopgemerkt blijven en zal waarschijnlijk in de publiciteit komen met de nodige imagoschade tot gevolg. Uw website is een walvis op het grote internet: niet alleen kunt u slachtoffer worden van walvisjagers, maar door uw grootte (risicoprofiel) alleen al trekt u de aandacht van anderen.

Bovenop de security-maatregelen voor de profielen Guppy en Tonijn, moet u ook denken aan:

- **Privacy:** Regel uitgebreide bescherming van persoonsgegevens, denk aan het separaat opslaan van de klantgegevens in een apart systeem, zorg voor encryptie op die gegevens en denk ook aan het encrypten van back-ups van deze gegevens
- **Payment:** Zorg voor redundancy op het vlak van betalingsverkeer. Waarschijnlijk heeft uw payment-provider daar oplossingen voor, maar overweeg ook zeker om te werken met een tweede payment-provider die het betalingsverkeer kan overnemen
- **Continuïteit:** Uw webshop is dermate belangrijk, dat uitval voorkomen moet worden. Zorg ervoor dat uw online omgeving redundant is uitgevoerd op twee fysieke locaties. Voor traditionele hosting betekent dat twee verschillende datacenters, voor cloud computing meerdere availability zones
- **Reputatie:** stel een uitgebreid communicatieplan op richting uw klanten en (offline/online) media, dat kan worden uitgevoerd op het moment dat u reputatieschade dreigt te ondervinden van onbeschikbaarheid, foute content of diefstal van gegevens uit uw online omgeving.

1.3 Overige risico's en bedreigingen

Aanvullend op bovengenoemde maatregelen die gekoppeld zijn aan de risicoprofielen, is het ook verstandig om rekening te houden met de volgende zaken:

- **Cookiewet:** U mag niet zomaar cookies plaatsen. Zijn er cookies die niet strikt noodzakelijk voor het functioneren van uw webshop (analytics, profiling), dan moet u in ieder geval uw bezoekers hierover informeren en expliciet toestemming vragen alvorens de cookies te plaatsen[4]
- **EU-wetgeving:** Als u vestigingen buiten de EU heeft of uw data buiten de EU opslaat, moeten aanvullende maatregelen worden getroffen om de privacy van persoonsgegevens te waarborgen. Denk hierbij aan 'safe harbour'-overeenkomsten.[5]
- **Opslag wachtwoorden:** Wachtwoorden van uw klanten moeten nooit leesbaar worden opgeslagen binnen uw webshop. Zorg ervoor dat wachtwoorden via moderne hashing[6] en salting[7] worden beschermd, zodat bij een mogelijke inbraak de wachtwoorden onbruikbaar zijn
- **Privacywetten:** Sla alleen die privacygevoelige gegevens op die noodzakelijk zijn voor het functioneren van de webshop. Wees voorzichtig met het mailen van deze data. Voor aanvullende privacy-data of ander gebruik dan voor het oorspronkelijk beoogde doel moet expliciet toestemming worden gevraagd
- **Creditcards:** Voor het gebruik van creditcards gelden specifieke normen[8] (PA-DSS voor software en PCI-DSS voor infrastructuren). Zorg ervoor dat de payment-provider, uw webshop en de online infrastructuur aan deze standaarden voldoen

REFERENTIES

[4] *http://nl.wikipedia.org/wiki/Cookie_%28internet%29#Nederlandse_cookiewetgeving*
[5] *http://en.wikipedia.org/wiki/Safe_harbor_%28law%29*
[6] *http://en.wikipedia.org/wiki/Hash_function*
[7] *http://en.wikipedia.org/wiki/Salt_%28cryptography%29*
[8] *https://www.pcisecuritystandards.org/security_standards/documents.php*

- **Uitbesteding:** Als u het development/beheer van uw webshop uitbesteedt, zorg er dan voor dat eigendom van de code en gegevens goed belegd zijn in de overeenkomsten met de ICT-toeleveranciers. Controleer op certificeringen (zoals ISO 27001). Overweeg ESCROW voor code[9]
- **Security-patches:** Maak over het installeren van security-patches afspraken met de beheerder van uw webshop. Denk niet alleen aan patches op standaard software, maar ook aan bugfixes van maatwerk. Houdt tevens 'End-Of-Life'-verklaringen[10] in de gaten, zodat u tijdig kunt updaten
- **Secure connections:** Als u privacygevoelige gegevens van uw bezoekers opvraagt, uitwisselt of toont, moet dit over een veilige verbinding gebeuren (HTTPS[11]). Gebruik hierbij altijd up-to-date standaarden en protocollen (zo is SSL3.0[12] of SHA-1[13] niet meer veilig).

Hieronder staan alle maatregelen aangaande het Digitale Dreigingen Model beknopt weergegeven, uitgesplitst naar risicoprofiel:

Onderwerpen	Guppy (13-29 punten)	Tonijn (30-47 punten)	Walvis (48-65 punten)	Tips & Tricks
Privacy	Bewerkersover-eenkomst met toeleveranciers	Regelmatig toetsing security & secure development	Encrypt data op site, inclusief backups	- Cookiewet / privacywetgeving - EU privacywetgeving - Versleutelen van wachtwoorden - Verzenden gegevens per e-mail - Creditcards - Uitbesteding - Denk aan eigendom gegevens - Beveiligingsevaluatie / penetratietesten - Secure connections - Security patches - Dataminimalisatie
Payment	Zorg voor sluitende financiële administratie	SLA met payment provider	Redundancy betalingsverkeer	
Continuïteit	Standaard SaaS webshopdienst	Professionele hostingpartij, managed services, secure development	Twee datacenters, DDoS, IDS/IPS	
Reputatie	Communicatie buiten de website om (twitter/ facebook)	Tref maatregelen tegen uitval, onjuiste gegevens of datalekken	Zorg voor een communicatieplan	

Tips & tricks per risicoprofiel

REFERENTIES

[9] *http://en.wikipedia.org/wiki/Escrow*
[10] *http://en.wikipedia.org/wiki/End-of-life_%28product%29#Computing*
[11] *http://en.wikipedia.org/wiki/Transport_Layer_Security*
[12] *http://en.wikipedia.org/wiki/Transport_Layer_Security#POODLE_attack*
[13] *http://en.wikipedia.org/wiki/SHA-1*

2. Veilige hosting: wat kunt u uitbesteden?

Bij het kiezen van een betrouwbare hostingpartij om uw webshop onder te brengen kunt u gebruik maken van de onderstaande checklist. Buiten een goede prijs is een goede dienstverlening omtrent de veiligheid van webshops natuurlijk ook heel belangrijk. Een goede hoster neemt doorgaans een (groot) deel van de zorgen uit handen. Daarbij valt te denken aan de volgende zaken:

Maatregelen tegen hackers

- Automatische en regelmatige updates van software, niet alleen van uw besturingssysteem, maar ook van uw webshop en aanvullende software
- Versleutelen van gegevens, met name persoonsgegevens
- Hhet maken van een dagelijkse backup op een veilige plek (niet op de server zelf dus!)
- 24-uurs alarmering bij hacks en hackpogingen
- 'Intrusion Prevention'-systemen, dus het vooraf goed dichtzetten van systemen en het continu bewaken en beveiligen tegen hackpogingen.

Maatregelen tegen DDoS-aanvallen

- Niet alleen voor uw server, maar voor het hele netwerk van de hoster.

Goede processen en procedures omtrent informatiebeveiliging, service en kwaliteit

- Denk aan certificering volgens ISO 27001, ISO 9001, ISAE 3402 en ISO 20000
- Let op dat het hebben van een ISO-certificaat niet altijd betekent dat uw webshop ook veilig is. Het ligt aan welke (aanvullende) diensten u afneemt
- Controleer dus altijd welke diensten wel en niet in uw abonnementsbedrag zijn inbegrepen.

Gevraagd en ongevraagd advies over het beter beveiligen van uw webshop

- Een goede hoster brengt u proactief op de hoogte van de actuele stand van zaken
- Heeft uw hostingpartner misschien een service die u automatisch attendeert op belangrijke veiligheidsincidenten?
- Ga er niet vanuit dat veiligheid en beveiliging van uw webshop uitsluitend bij de hoster ligt. Stem goed af wie wat doet. Vraag om rapporten omtrent de beveiliging van uw shop
- Heeft uw hostingpartner een dienst die actief uw shop scant op 'gaten' en verbeterpunten omtrent beveiliging? Vraag erom, of vraag Thuiswinkel.org om advies.

Tot slot: neem niet aan dat in elk hostingabonnement alle beveiligingsmaatregelen 'inclusief' zijn. Vraag de hoster altijd om specificaties en uitleg. Sowieso is het de eigen verantwoordelijkheid van webshop-eigenaars om vooraf een risico-analyse te maken van de online veiligheid. Als u die expertise niet in huis heeft, is het aan te raden hiervoor aan te kloppen bij security-specialisten, ICT-leveranciers of het eigen hostingbedrijf.

Meer lezen?

Op ShoppingTomorrow.nl vindt u meer informatie over Online Security & Hosting.

ShoppingTomorrow/
Online Security & Hosting

GASTHEER

Ludo Baauw

Directeur

Intermax

Ludo@intermax.nl

VOORZITTER

John Hermans

Partner

KPMG

hermans.john@kpmg.nl

LEDEN EXPERTGROEP

Stan Hegt
Manager
KPMG

Roland van Kortenhof
Manager Operations
Thuiswinkel.org

Menno Borst
IT Risk Manager
IT Risk Retail (voorheen Maxeda)

Leendert van Duijn
CIO Benelux
Teleperformance

Sander Nieuwenhuis
Security Manager
Mirabeau

Ivan de Wit
Junior Advisor
KPMG

Robert van Manen
Directeur
Forus-P bv

Erik Roest
IT Manager
HotelSpecials.nl