Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Help! Mijn website is beklad

Wat kunt u doen tegen defacements?

Factsheet FS-2015-01
versie 1.0 | 4 maart 2015

Bij een defacement of digitale bekladding van een website verandert een aanvaller de inhoud van bestaande pagina's of plaatst nieuwe pagina's. Defacements van websites vinden dagelijks honderden keren plaats en zijn vaak ongericht.

In toenemende mate wordt bij de uitvoering van defacements malware achtergelaten, waardoor bezoekers van de website besmet kunnen raken. Het is dan ook van belang de afhandeling van en communicatie bij een defacement goed voor te bereiden.

Veel websites zijn vatbaar voor eenvoudig te voorkomen defacements. U kunt diverse maatregelen nemen om het risico op een defacement aanzienlijk te verkleinen.

In deze factsheet vindt u de belangrijkste kenmerken van een defacement, leest u wat de gevolgen kunnen zijn en hoe u zich er zo goed mogelijk tegen kunt wapenen.

Doelgroep
Deze factsheet richt zich op eigenaren, ontwikkelaars en beheerders van websites.
Bent u eigenaar van een website maar heeft u de ontwikkeling en/of het beheer van uw website uitbesteed, treed dan in overleg met uw leveranciers over hoe u zich gezamenlijk tegen deze vorm van misbruik kunt wapenen.

De belangrijkste feiten

- Bij een defacement verandert een aanvaller de inhoud van een website.
- Defacements zijn veel voorkomend en meestal het gevolg van een inbraak op uw CMS of webserver.
- Aanvallers gebruiken defacements om malware te verspreiden.
- Door websites goed te beheren te en beveiligen neemt het risico op een defacement af.
- Een goed voorbereide respons zorgt voor een sneller herstel van een defacement.

Wat is een defacement?

Bij een defacement of digitale bekladding van een website verandert een aanvaller de inhoud van bestaande pagina's of plaatst nieuwe pagina's. Dit kan zeer opvallend gebeuren of juist niet. Een defacement is vaak het gevolg van een inbraak op een CMS[1] of een webserver, bijvoorbeeld door misbruik van een kwetsbaarheid of van een bestaand gebruikersaccount en wachtwoord .

Defacements kunnen specifiek op een bepaalde organisatie gericht zijn, maar zijn in verreweg de meest voorkomende gevallen ongericht. Ongerichte, geautomatiseerde defacements kunnen in één keer grote hoeveelheden websites aanpassen. Dergelijke defacements vinden wereldwijd dagelijks honderden keren plaats[2].

Een defacement kan ook onopvallend worden uitgevoerd. Een aanvaller kan bijvoorbeeld één artikel toevoegen of aanpassen op een nieuwssite, waardoor niet direct opvalt dat de site is aangepast, en op die manier trachten een boodschap over te brengen. Daarnaast kan een website door een defacement ook misbruikt worden als distributiepunt voor malware.

Er kunnen ook andere aanleidingen zijn waardoor een bezoeker van een website niet de juiste content krijgt gepresenteerd, bijvoorbeeld vanwege een zogenaamde DNS hijack[3]. Hierbij wordt de gebruiker bij het opvragen van een webpagina naar een valse pagina geleid. Hoewel dit 'officieel' niet als een defacement wordt geclassificeerd, kunnen de gevolgen wel gelijk zijn[4].

[1] Een content management system (CMS) is software die wordt gebruikt om de inhoud van een website te beheren. Voorbeelden van veelgebruikte CMS-en zijn Joomla!, WordPress en Drupal.
[2] www.zone-h.org registreert maandelijks tussen de 50.000 en 100.000 website defacements.
[3] Domain Name System, de service waarmee op internet een domeinnaam (zoals www.ncsc.nl) wordt vertaald naar het bijbehorende IP-adres.
[4] Voor een voorbeeld hiervan: http://www.esecurityplanet.com/hackers/hackers-deface-malaysia-airlines-website.html

Wie voeren defacements uit en waarom?

Hackers, scriptkiddies of cybervandalen voeren vaak defacements uit 'omdat het kan'. Ze scannen geautomatiseerd het internet af op zoek naar websites die kwetsbaarheden vertonen en veranderen vervolgens automatisch de voorpagina van dergelijke websites met een eigen pagina, een zogenaamde 'mass defacement'.

Deze vorm van defacement is een soort digitale graffiti, waarbij de hacker zijn 'tag' achterlaat. Op internet zijn ranglijsten waarop wordt bijgehouden hoeveel websites iemand beklad heeft. Iedere geslaagde defacement is goed voor het imago.

1 Voorbeeld van een *tag*.

Hacktivisten zoals Anonymous of hackergroepen als de Syrian Electronic Army voeren defacements uit om hun ideologische boodschap over te brengen of tegenstanders te saboteren.
In veel gevallen wordt alleen getracht zo veel mogelijk websites uit een bepaald land of van een bepaald type organisatie te defacen en zo de ideologische boodschap te verspreiden.

2 Voorbeeld van een ideologische defacement.

Cybercriminelen kunnen, met financieel gewin als oogmerk, een website aanpassen om malware te verspreiden, inloggegevens te stelen of het onderdeel van een botnet te laten uitmaken. Ook hier zal de dader trachten dit onopvallend te doen, zodat de site zo lang mogelijk gecompromitteerd kan blijven. Ook het plaatsen van met malware besmette advertenties op bonafide websites is een groeiend fenomeen.

Ten slotte kunnen ook ontevreden oud-medewerkers hun ongenoegen uiten door de website van hun vroegere werkgever te defacen. Zij kunnen nog steeds beschikken over de kennis, zoals gebruikersnamen en wachtwoorden, waarmee ze de website eenvoudig kunnen aanpassen.

Hoe ernstig is een defacement?

De gevolgen van een defacement kunnen voor iedere organisatie verschillen. Een organisatie moet zelf de impact van een mogelijke defacement inschatten en op basis daarvan maatregelen bepalen. Een defacement van een website leidt in eerste instantie vooral tot imagoschade en de kosten voor het herstellen van de website. Bedrijven die voor hun bedrijfsvoering afhankelijk zijn van hun website kunnen door een defacement ook financiële schade door gemiste omzet leiden.

Een defacement raakt in het algemeen de achterliggende computersystemen van een organisatie niet, maar kan wel worden gebruikt om af te leiden van andere vormen van cybercriminaliteit. Daarnaast kunnen cybercriminelen defacements gebruiken om medewerkers inloggegevens tot bijvoorbeeld de webmailomgeving van een organisatie afhandig te maken, waarbij gebruik wordt gemaakt van de domeinnaam van de organisatie.

Wanneer een defacement gebruikt wordt om malware te verspreiden of om bezoekers van de site te verleiden om hun inloggegevens voor de site of authenticatieservices zoals Facebook, Google of DigiD in te vullen, gaat de schade verder dan alleen het getroffen bedrijf. In dat geval kan persoonlijke informatie van bezoekers of bedrijfsinformatie worden buitgemaakt.

Wanneer ben ik kwetsbaar?

Een website is kwetsbaar voor defacements wanneer:

- de (virtuele) webserver of de VPS-interface[5] niet op een veilige manier is ingericht. Wanneer door onbevoegden toegang tot de webserver of de VPS kan worden verkregen, hebben zij de mogelijkheid content van de website toe te voegen, aan te passen of te verwijderen;
- het CMS (of CMS-plugins) kwetsbaarheden bevat. De meeste CMS-leveranciers publiceren regelmatig security-updates van hun product, waarin nieuw ontdekte kwetsbaarheden zijn opgelost;
- inloggegevens voor het CMS of de webserver in handen van aanvallers terecht zijn gekomen, bijvoorbeeld door gebruik van standaard accounts en wachtwoorden, via gerichte phishing e-mails[6] of omdat de website geen gebruik maakt van TLS[7] om vertrouwelijke informatie uit te wisselen;
- de inrichting van de website kwetsbaarheden bevat, zoals XSS[8], waarmee 'valse' inhoud kan worden voorgeschoteld;
- door onbetrouwbare advertentieleveranciers malware op de website wordt geplaatst.

[5] Met virtual private servers (VPS) kunnen op een fysieke webserver meerdere logisch gescheiden virtuele servers worden gecreëerd.
[6] Phishing emails zijn misleidende emails die een link bevatten naar een malafide website of met kwaadwillende software.
[7] TLS – Transport Layer Security, een protocol voor het opzetten en gebruiken van een cryptografisch beveiligde verbinding tussen twee computersystemen. Voor meer informatie, zie https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html.
[8] Cross Site Scripting (XSS) is een aanvalsmethode waarmee onder meer valse content aan een gebruiker kan worden gepresenteerd. Zie ook https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29.

De websites van bepaalde typen van organisaties kennen een extra risico op gerichte aanvallen, bijvoorbeeld religieuze en politieke organisaties en mediabedrijven. Wanneer een dergelijke organisatie getroffen wordt door een defacement, hoeft dit echter niet altijd een gerichte aanval te betekenen en is de kans groot dat de getroffen website medeslachtoffer is van een mass defacement.

Defacement van social media

Voor organisaties die gebruik maken van social media zoals Twitter en Facebook, is het zaak na te denken over de gevolgen van misbruik van deze middelen. Vervalste berichten op Twitter of een aangepaste profielpagina op Facebook kunnen een even grote impact hebben op het imago als een defacement van de website.

Als gebruiker heeft u weinig invloed op de beveiligingsinrichting van grote social media sites, maar u kunt zich wel zo goed mogelijk wapenen tegen een eventueel misbruik van uw gebruikersaccount:

» Maak waar mogelijk gebruik van 2-factor authenticatie.
» Wijzig wachtwoorden regelmatig, ook wanneer personen die toegang hebben tot de accounts de organisatie verlaten.
» Ook hier geldt: maak een responsplan.

Hoe merk ik een defacement op?

De meeste defacements zijn zó opvallend, dat er geen onduidelijkheid bestaat dat de site is gedefacet en wie de verantwoordelijkheid claimt. Er zijn diverse technische maatregelen te treffen om uw website te monitoren op ongeautoriseerde wijzigingen. Er zijn ook bedrijven die dit, tegen betaling, voor u doen.

Als u een defacement niet direct zelf opmerkt, kunt u ook gewaarschuwd worden door:

» gebruikers die de site bezoeken en de defacement melden;
» databases op internet die defacements registreren en in sommige gevallen een bericht naar de websitebeheerder sturen;
» het monitoren van publieke uitlatingen over uw website op sociale media zoals Twitter;
» uw internet service provider, die vaak als eerste wordt gewaarschuwd bij geconstateerd misbruik van uw website.

Hoe voorkom ik een defacement?

Hoewel nooit met zekerheid te voorkomen is dat uw website wordt getroffen door een defacement, zijn er diverse preventieve maatregelen die u (of uw leverancier) kunt nemen om het risico hierop aanzienlijk terug te brengen.

» Zorg voor een robuust ingerichte server, waarop geen onnodige services zijn geïnstalleerd.
» Installeer altijd de laatste patches en security-updates op uw systeem.
» Controleer regelmatig of uw systeem nog up-to-date is en controleer hierbij ook op de aanwezigheid van malware.
» Maak geen gebruik van standaard accounts en wachtwoorden voor uw besturingssysteem of CMS.
» Verwijder direct gebruikersaccounts van medewerkers die de organisatie verlaten of geen toegang tot het CMS of de webserver meer nodig hebben.
» Plaats een firewall en filter het netwerkverkeer onder meer op verdachte patronen.
» Beperk het aantal IP-adressen dat toegang mag krijgen tot de webserver en het CMS.
» Benader het CMS alleen via een TLS-beveiligde verbinding.
» Beveilig waar mogelijk de toegang tot de webserver en het CMS met een 2-factor-authenticatiemiddel[9].
» Scan regelmatig het beveiligingsniveau van de site, bijvoorbeeld met geautomatiseerde scanners. Stem dit vooraf goed af met de beheerders of eigenaren van de website, zodat dit niet gezien wordt als een aanvalspoging.
» Voer een responsible disclosure beleid[10] in, zodat bonafide hackers gevonden kwetsbaarheden in uw website op een vertrouwelijke manier kunnen melden. U kunt deze kwetsbaarheden dan herstellen voordat anderen er misbruik van kunnen maken.
» Maak, wanneer uw website door een externe leverancier wordt gehost, duidelijke afspraken over de beveiliging van de website.

Daarnaast kunt u, zeker wanneer het belang van de website of het imago van de organisatie groot is of het risico op een defacement bovengemiddeld, overwegen om:

» periodiek een penetratietest[11] uit te voeren op de kwaliteit van de beveiliging van de website en geconstateerde kwetsbaarheden te repareren. Hiermee kunt u bijvoorbeeld de eerdergenoemde XSS-kwetsbaarheid detecteren;
» een Intrusion Detection System (IDS)[12] te implementeren om verdachte activiteiten sneller te detecteren.

Hoe bereid ik me voor op een defacement?

Omdat 100% garantie op veiligheid niet bestaat, moet u altijd voorbereid zijn om de schade na een defacement te kunnen beperken.

» Maak regelmatig een back-up van de site. Hiermee is het herstel van de site eenvoudiger.
» Zorg voor een representatieve, vervangende webpagina die snel geplaatst kan worden in geval van nood.
» Zorg voor een responsplan waarin staat wat te doen in geval van een defacement (zie de volgende paragraaf). Denk hierbij ook aan de interne en externe communicatie over het incident.
» Maak, wanneer de website door een externe leverancier wordt gehost, vooraf duidelijke afspraken over wat de leverancier op eigen initiatief mag/moet doen en wat eerst met opdrachtgever moet worden afgestemd.

[9] Bij 2-factor authenticatie wordt naast een wachtwoord een tweede authenticatiemiddel, bijvoorbeeld een verificatiecode per sms, gebruikt.
[10] Voor meer informatie, zie: https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html.
[11] Voor meer informatie, zie https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/pentesten-doe-je-zo.html.
[12] Voor meer informatie, zie https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/intrusion-detection-system.html.

De belangrijkste maatregelen tegen een defacement op een rijtje

Voorkomen:

1. Zorg dat uw webserver en CMS op een veilige manier zijn ingericht en installeer altijd de laatste beveiligingsupdates.
2. Maak waar mogelijk gebruik van 2-factor authenticatie voor toegang tot uw webserver en CMS.

Voorbereiden:

3. Maak regelmatig een back-up van uw site.
4. Stel een responsplan op, waarin u vastlegt wat te doen in geval van een defacement.

Herstellen:

5. Plaats een vervangende webpagina.
6. Communiceer intern en extern tijdig over het incident en de mogelijke gevolgen.
7. Stel de gecompromitteerde content veilig in verband met een strafrechtelijk onderzoek en doe aangifte bij de politie.
8. Richt uw website opnieuw in en controleer voorafgaand aan publicatie zorgvuldig de beveiligingsinstellingen.
9. Onderzoek waar u verbeteringen kunt aanbrengen in de inrichting of het beheer van de site of de incident respons en voer de onderkende verbeteringen door.

Hoe herstel ik na een defacement?

Wanneer een defacement is geconstateerd, wordt het opgestelde responsplan uitgevoerd.

Voor het herstel op korte termijn is daarin opgenomen:

- Plaats een vervangende, representatieve webpagina.
- Bepaal welke schade de defacement met zich meebrengt. Is alleen het uiterlijk van de site gewijzigd of heeft de aanvaller ook malware of illegale content achtergelaten?
- Communiceer met de benodigde partijen over het voorval.
- Stel in verband met een eventueel strafrechtelijk onderzoek de content en de logging van de aangevallen site veilig.
- Probeer te achterhalen hoe de defacement is uitgevoerd, welke kwetsbaarheden zijn misbruikt.
- Controleer de meest recente back-up van de site op de aanwezigheid van malware en kwetsbaarheden.
- Richt een nieuwe server in met de laatste versies van de benodigde software en zet hier de meest recente, veilige back-up van de inhoud van de site op.
- Publiceer de nieuw ingerichte site, zodra duidelijk is dat alle kwetsbaarheden zijn verholpen.

Wanneer de website weer hersteld is, zijn er nog de nodige zaken die op de langere termijn voor definitief herstel moeten zorgen:

- Doe altijd aangifte[13] bij de politie.
- Onderzoek welke technische kwetsbaarheden de website nog kent. Repareer deze of bouw de website opnieuw met minder kwetsbare producten.
- Onderzoek of het beheer van de website verbeteringen nodig heeft. Denk hierbij bijvoorbeeld aan de tijdige installatie van patches en updates, de monitoring van de site en de respons van de organisatie bij het incident.
- Overweeg, als u de website zelf beheert of ontevreden bent over de mogelijkheden die uw huidige leverancier biedt, om de hosting bij een andere leverancier onder te brengen.
- Evalueer het responsplan. Wat ging goed en wat verliep niet naar wens? Moet het responsplan in de toekomst (vaker) getest worden? Zijn er extra of juist minder maatregelen nodig?
- Wanneer u in het bovenstaande structurele verbeteringen heeft onderkend, ga dan actief aan de slag met de uitvoering hiervan.

Tot slot:

Defacements van websites worden steeds meer een propagandamiddel van ideologisch geïnspireerde groeperingen. Daarnaast komen er meer middelen beschikbaar waarmee websites automatisch worden gescand en bij een gevonden kwetsbaarheid automatisch worden aangepast.
Door gerichte beveiligingsmaatregelen te treffen kunt u het risico op een defacement aanzienlijk verkleinen.

Om organisaties minder kwetsbaar te laten zijn voor deze en andere aanvallen heeft het NCSC 'ICT-beveiligingsrichtlijnen voor webapplicaties'[14] gepubliceerd.

Meer factsheets en richtlijnen over de beveiliging van uw websites, vindt u op www.ncsc.nl:

- ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS);
- Whitepaper Pentesten doe je zo;
- Whitepaper Intrusion Detection system;
- Factsheet HTTPS kan een stuk veiliger.

[13] Voor meer informatie, zie https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/handreiking-cybercrime.html
Een ideologische defacement kunt u ook melden bij de AIVD, www.aivd.nl.

[14] Voor meer informatie, zie https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

Uitgave van **Nationaal Cyber Security Centrum**
Tot stand gekomen in samenwerking met **SIDN** en **AIVD**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55 | F 070-322 25 37
Publicatienr: FS-2015-01 | Aan deze informatie kunnen geen rechten worden ontleend.