Stefanie Weber

Copywriter - Vertaler - Content Creator

Portfolio

Tijdens mijn werkzaamheden ben ik grotendeels verantwoordelijk geweest voor de content van het blog van mijn werkgever. In dit portfolio heb ik een greep uit mijn jarenlange ervaring samengevoegd om een beeld te geven van mijn kunnen als blogger, tekstschrijver en editor.

Wilt u meer weten? Neem dan even contact met mij op via e-mail of telefoon. Ik geef graag achtergrondinformatie over mijn schrijfstijl en werkwijze.

Inhoud

Contact

info@stefanieweber.nl

06-539 11 899

Polderpeil 390
2408SG Alphen a/d Rijn

13 maart 1988

Rijbewijs B

Stefanie Weber

Copywriter - Vertaler - Content Creator

Dit artikel verscheen op 23 april 2019 en is geschreven naar aanleiding van aangekondigde nieuwe richtlijnen van het Nationaal Cyber Security Centrum voor gebruik van het TLS protocol. Ik heb voor dit artikel de richtlijnen van het NCSC uitgebreid doorgelezen, maar ook geput uit eerdere oudere blogartikelen die dieper op de stof ingaan.

Het originele artikel is hier te vinden:

https://blog.networking4all.com/2019/04/ncsc-publiceert-nieuwe-richtlijnen-voor-tls/

NCSC publiceert nieuwe richtlijnen voor TLS

Het Nationaal Cyber Security Centrum, onderdeel van het Ministerie van Justitie en Veiligheid, publiceert vandaag de vernieuwde beveiligingsrichtlijnen voor TLS. In dit document stelt het NCSC welke TLS configuraties er klaar zijn voor de toekomst, en welke configuraties verouderd zijn en een potentieel gevaar vormen. Hierbij is vooral aandacht besteed aan TLS 1.3, dat in augustus 2018 is geïntroduceerd.

Het document van het NCSC bevat duidelijk gebruiksadvies voor beheerders om een veilige configuratie op te zetten. Hierbij wordt gekeken naar de meest veilige algoritmes en hoe deze het beste te gebruiken zijn. Eén van de adviezen is om rekening te houden met mogelijk verouderde software die nog steeds in gebruik is. Instellingen zijn ingedeeld in de categorieën ‘goed’, ‘voldoende’, ‘uit te faseren’ en ‘onvoldoende’.

Een instelling die ‘onvoldoende’ veilig is volgens het NCSC moet niet gebruikt worden. Instellingen die zijn gemarkeerd als ‘uit te faseren’ zijn een potentieel cybersecurity gevaar met het oog op de huidige ontwikkeling van aanvalstechnieken. Voor sommige bedrijven zijn deze instellingen echter nog noodzakelijk omdat zij gebruikmaken van verouderde applicaties die niet vervangen kunnen worden. Het NCSC waarschuwt wel deze applicaties alleen nog te blijven gebruiken als de uitfasering ervan al op de agenda staat.

Voldoende of goede instellingen worden, niet geheel verrassend, aanbevolen door het NCSC. Wanneer u zelf het beheer van uw SSL certificaten in handen hebt, zou u daarom waar mogelijk alleen moeten kiezen voor goede instellingen, en wanneer dat niet mogelijk blijkt, moeten kijken naar instellingen die de waarde ‘voldoende’ hebben.

Het advies nader bekeken

In het advies van het NCSC wordt, om te beginnen, het gebruik van TLS 1.3 aanbevolen. De veiligheid van een TLS-verbinding is afhankelijk van het gebruikte algoritme. Het advies van het NCSC is om uitsluitend algoritmes te gebruiken die voor forward secrecy zorgen. De beste keuze valt daarom dus op ECC-algoritmes voor zowel sleuteluitwisseling als certificaatverificatie. Het is ook belangrijk om te letten op de hashmethode: SHA-1 wordt simpelweg niet meer geaccepteerd. TLS 1.3 ondersteunt daarnaast ook andere meer kwetsbare hash-methodes zoals SHA-224 en MD5 niet meer.

Daarnaast geeft het NCSC ook minder bindend advies, waar u aan kunt voldoen door simpelweg over te stappen op het gebruik van TLS 1.3. Zo is compressie standaard uitgeschakeld en maakt TLS 1.3 al standaard gebruik van 0-RTT of Zero Round Trip Time. Ten slotte geeft het NCSC ook het advies mee om gebruik te maken van OCSP Stapling.

Download de richtlijnen

Het volledige document van het Nationaal Cyber Security Centrum is te downloaden vanaf hun website. Heeft u naar aanleiding van dit bericht nog vragen, stel ze dan gerust via support@networking4all.com of bel ons via (0)20 788 1030. We helpen u graag verder.

Stefanie Weber

Copywriter - Vertaler - Content Creator

In dit artikel ben ik de diepte ingedoken, omdat TLS 1.3 ongeveer een maand voor publicatie officieel was goedgekeurd als de nieuwe standaard voor het TLS protocol en ik benieuwd was wat er nou eigenlijk anders aan was. Ik heb voor dit artikel samengewerkt met onze security specialist, maar me daarnaast ook ingelezen in de RFC.

Het originele artikel is hier te vinden: https://blog.networking4all.com/2018/09/een-sprong-vooruit-met-tls-1-3/

Een sprong vooruit met TLS 1.3

Dat de ontwikkelingen omtrent het internet nooit stilstaan is zowel een vloek als een zegen. Toen SSL 2.0 werd geïntroduceerd in 1995, nadat 1.0 al nooit werd uitgebracht vanwege onoverkomelijke security problemen in het protocol, zullen de ontwikkelaars waarschijnlijk niet gedacht hebben dat het slechts een jaar later al vervangen zou worden door versie 3.0. Inmiddels zijn we 3 versies van het protocol verder en aanbeland bij TLS 1.2. Maar deze editie van het securityprotocol werd alweer 10 jaar geleden, in augustus 2008, gelanceerd, en werd sinds de lancering geplaagd door vulnerabilities die steeds weer zwakke punten wisten bloot te leggen. Hoog tijd voor een upgrade, dus?

TLS 1.3 werd in augustus van dit jaar officieel gedefinieerd in RFC 8446 als de nieuwe standaard voor het TLS-protocol. Er zijn een hoop veranderingen doorgevoerd in deze nieuwe versie die het waard zijn om eens onder de loep te nemen.

Sneller, beter, sterker

Om te beginnen is er in versie 1.3 wat overbodig werk weggehaald: tijdens de client hello wordt nu ook meteen een key share meegestuurd. Hiervoor waren dit twee aparte stappen, waar dus ook twee keer een request en response voor nodig waren. Met de toevoeging van Zero Round Trip Time (0-RTT), een methode waarbij TLS 1.3 het sessieticket van een eerder bezochte webserver onthoudt, kan het proces zelfs nog een stap worden ingekort. TLS 1.3 is hiermee dus sneller dan 1.2.

Versie 1.3 ondersteunt ook niet langer oude, achterhaalde, of simpelweg te kwetsbare cipher suites, Elliptic Curves en hash-functionaliteit. Zo is ondersteuning voor SHA224 en MD5 verwijderd, en wordt Perfect Forward Secrecy of PFS tegenwoordig verplicht gesteld waardoor statische RSA en Diffie-Helmann key exchanges niet meer mogelijk zijn. Ook heeft TLS 1.3 resumption vervangen door een systeem van tickets in combinatie met pre-shared keys, of PSK.

Daarnaast is compressie uitgeschakeld. Compressie houdt in dat de data die verstuurd wordt via TLS samengepakt wordt om het dataverkeer te verlagen. Het nadeel van compressie is wel, dat die data steeds weer in- en uitgepakt moet worden voor het verwerkt kan worden, wat de druk op de CPU verhoogt. HTTP kent ook een compressieproces dat vergelijkbaar werkt en een aantal jaar geleden de basis was voor de BREACH-vulnerability. Met het uitschakelen van compressie wordt weliswaar het dataverkeer hoger, maar is de druk op de CPU wel constant.

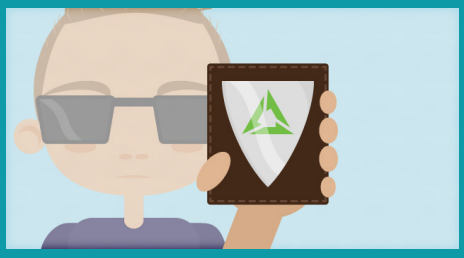
De aanpassingen in TLS 1.3 zorgen er onder andere voor dat vulnerabilities als LogJam, Freak, CRIME, SLOTH, DROWN, Poodle, en Lucky13 niet meer van toepassing zijn.

Toepassen

Hoewel de RFC officieel geïntroduceerd is, betekent dit nog niet automatisch dat TLS 1.2 uitgefaseerd is en niet meer gebruikt wordt. TLS 1.3 is nog bij lange na niet overal geïmplementeerd. Het is daarom niet aan te raden om uw server al alleen om te zetten naar TLS 1.3. Wat wel een mogelijkheid is, is het toevoegen van TLS 1.3 aan uw configuratie. Als u zelf wilt experimenteren met TLS 1.3, kunt u het installeren op uw server. Onze Product Manager Security, Sebastian Broekhoven, heeft een uitgebreide omschrijving gemaakt voor de installatie van TLS 1.3 op Nginx 1.15.2 met OpenSSL 1.1.1-pre8. Hierin legt hij exact uit welke stappen hij heeft ondernomen om de installatie te voltooien.

Stefanie Weber

Copywriter - Vertaler - Content Creator



Naast in-depth artikelen was het natuurlijk mijn taak om ons bedrijf en onze dienstverlening te verkopen. Dit artikel is gepubliceerd nadat wij securitydiensten aan ons portfolio toe hadden gevoegd.

Het originele artikel is hier te vinden:

https://blog.networking4all.com/2018/05/security-op-maat-securitydiensten-networking4all/

Security op maat met de securitydiensten van Networking4all

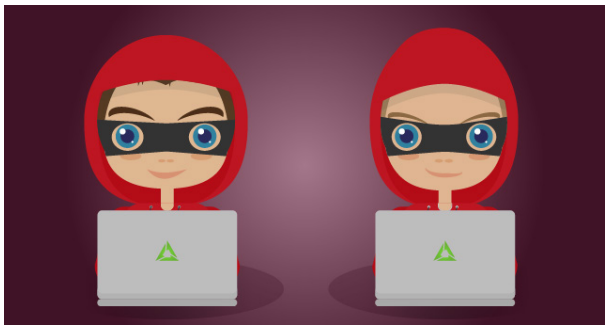
Een bedrijf dat tegenwoordig niet het merendeel van haar zaken doet via het internet, dat komt bijna niet meer voor. Daarom is het belangrijk dat elk bedrijf, hoe klein of groot ook, er voor zorgt dat de beveiliging van hun online systemen goed op orde is. Met de aanscherping van de privacywetgeving in Europa in het achterhoofd is goede beveiliging van data helemaal een must. Networking4all onderschat het belang van goede beveiliging niet, en biedt daarom vanaf nu meerdere security diensten die uw bedrijf kunnen helpen met het opwaarderen en optimaliseren van uw beveiliging.

Vulnerability scan
De Vulnerability Scan is een globale scan die uw netwerk, applicatie of systeem controleert tegen bekende vulnerabilities en security problemen, zoals de OWASP Top Ten. Onze security consultants lopen vervolgens de gevonden vulnerabilities met de hand na en bekijken of, en in hoeverre, de vulnerability te misbruiken is. Deze gevonden resultaten worden gebundeld in een rapport, met bijbehorend advies over het oplossen van de problemen, waarmee u aan de slag kunt. De vulnerability scan is een ideaal product voor zowel kleine ondernemers en ZZP'ers als grote multinationals, omdat het snel uit te voeren is en een behapbaar resultaat geeft. Regelmatig een vulnerability scan uitvoeren geeft daarom een goed inzicht in uw security.

Penetratietest
Maar alleen weten dat er een kwetsbaarheid in uw systeem of netwerk zit is soms niet genoeg. Zeker wanneer u kwetsbaarheden blijkt te hebben waar, mocht er misbruik van gemaakt kunnen worden, uw bedrijf mogelijk flinke schade van kan oplopen. Het zou ten slotte voor kunnen komen dat een hacker via een onopgemerkte achterdeur binnen is gekomen en er vandoor is gegaan met gegevens van klanten, betalingsgegevens, of bedrijfsgevoelige informatie zoals recepten, beleidsdocumenten of contracten.

Om vast te kunnen stellen welke data op de tocht komt te liggen wanneer een hacker binnen weet te komen in uw netwerk, kunt u onze security consultants een penetratietest laten uitvoeren. Tijdens deze test wordt er onder uw toezicht bij u ingebroken en aantoonbaar gemaakt welke gegevens zij hebben weten te bemachtigen. Samen met onze consultants kunt u vervolgens aan de slag met het verbeteren van uw security.

De penetratietest kan zowel op afstand als op locatie worden uitgevoerd. Tijdens een test op locatie kan bijvoorbeeld ook worden uitgezocht of uw kantoornetwerk van buitenaf bereikbaar is, of dat uw medewerkers gevoelige informatie openbaar laten staan door bijvoorbeeld niet hun werkplek af te sluiten wanneer ze weglopen of wachtwoorden laten slingeren.



Stefanie Weber

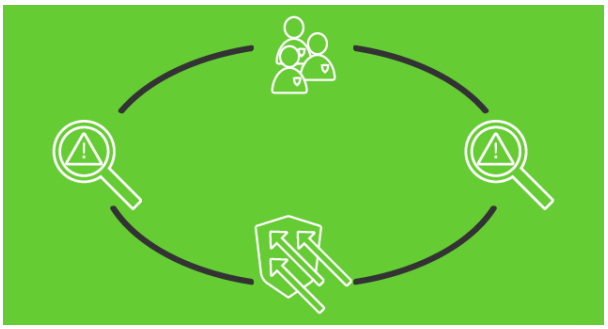
Copywriter - Vertaler - Content Creator

Red Teaming
De vulnerability scan en penetratietest bieden u een goed inzicht in uw security en geven duidelijk aan waar de gevoelige plekken liggen. Wat ze echter niet doen, is u inzicht geven in hoe uw personeel omgaat met een daadwerkelijke onverwachte bedreiging. Daar biedt Red Teaming uitkomst voor.

Red Teaming is een security assessment in de vorm van een realistische simulatie van een gecontroleerde cyberaanval. Tijdens deze aanval is het belangrijk dat zo min mogelijk medewerkers op de hoogte zijn van uw afspraken met ons security team. Zo krijgt u een accuraat inzicht in hoe zij reageren, en welke handelingen zij uitvoeren om de aanval af te slaan of de schade te beperken. Ons team begint met een vooronderzoek naar uw bedrijf, uw medewerkers, uw zakelijke contacten en uw klanten. Met de informatie die zij vanuit publieke bronnen kunnen verzamelen, vallen ze vervolgens uw bedrijf aan op drie vlakken: technologisch, fysiek, en sociaal.

Zo kan het bijvoorbeeld gebeuren dat ze proberen binnen te komen in uw kantoor, uw WIFI kraken, openstaande apparaten zoals de printer of de thermostaat hacken, of keyloggers installeren op computers van uw medewerkers. Maar ook social engineering zal worden ingezet om bijvoorbeeld inloggegevens of werkschema's te achterhalen.

Red Teaming is een effectieve assessment van uw beveiliging, zowel digitaal als fysiek, en van de oplettendheid en vaardigheid van uw medewerkers. Met de resultaten van de assessment op zak kunt u de zwakke punten van uw organisatie doeltreffend verbeteren.



Supercombo
De drie securitydiensten van Networking4all werken ook heel goed samen. Een Red Teaming assessment werkt het beste als uw bedrijf hem niet verwacht, en is daarom minder effectief als deze te vaak wordt uitgevoerd. Een penetratietest daarentegen kan wel vaker worden ingezet, zoals wanneer u een grote update heeft doorgevoerd aan uw systemen, netwerken of applicaties. De vulnerability scan kunt u regelmatig laten uitvoeren, zodat mogelijke nieuwe vulnerabilities op tijd worden opgemerkt en kunnen worden afgehandeld voordat ze een probleem vormen. Zo kunt u de combinatie van onze diensten inzetten om de security van uw bedrijf in topconditie te houden.

Wilt u meer weten over onze securitydiensten? Kijk dan op onze website voor meer informatie, of stuur een e-mail naar onze security consultants via security@networking4all.com.

Stefanie Weber

Copywriter - Vertaler - Content Creator

Behalve zelf schrijven herschreef ik ook artikelen van anderen, zoals dit artikel dat oorspronkelijk door CEO Frank Leest was geschreven. Zijn eerste versie was ruim 8 A4-tjes lang; ik heb geprobeerd om het wat bondiger te houden. Wel was het belangrijk om zijn stijl in het achterhoofd te houden, omdat dit artikel ook op zijn LinkedIn zou verschijnen.

Het originele artikel is hier te vinden:

https://blog.networking4all.com/2019/05/presenteer-jij-met-prezi-aan-de-hele-wereld/

Presenteer jij met Prezi aan de hele wereld?

Een presentatie geven? Vroeger deden we dat lokaal in een Powerpoint presentatie. Later gebruikten we Google Slides. Tegenwoordig is Prezi de tool waar iedereen naar grijpt. Met deze online presentatietool maak je makkelijk prachtige presentaties met effecten en grafische details die een statische Powerpoint presentatie van z'n levensdagen nog niet kan benaderen. Maar wat veel mensen zich niet realiseren, is dat de gratis versie van Prezi gewoon openbaar staat voor de wereld. Wanneer deze door Google is geïndexeerd komt deze naar boven als je met bepaalde zoekwoorden in de weer gaat. Met potentieel desastreuze gevolgen van dien.

En dat is precies wat ik deed: met een handjevol zoektermen en 30 minuten vrije tijd vond ik zeeën aan informatie. Omzetcijfers, winstmarges, salarissen van medewerkers, inclusief foto en bonussen. Ik vond bedrijfsstrategieën, marketingplannen, belangrijkste klanten met marges, persoonlijke informatie over medewerkers zoals resultaten van keuringen en onderzoeken. Er waren gegevens van telecombedrijven, recruitment agencies en uitzendbureaus, maar ook van de supermarkt om de hoek. Uiterst gevoelige informatie, open en bloot door die bedrijven zelf op het internet gezet. Bij nabellen van de gevonden informatie bleek dat deze mensen zelf ook niet door hebben gehad dat hun presentatie gewoon tevoorschijn kwam na een simpele Google zoektocht.

We doen het zelf

In tegenstelling tot wat je nu ongetwijfeld denkt, is dit geen lek, en is Prezi hier niet de boosdoener. In de voorwaarden van Prezi staat duidelijk vermeld dat de gratis versie, die standaard publiek staat, door iedereen ingezien kan en mag worden, waaronder zoekmachines en derden:

> "If you have a Prezi Public (free) account, all of the content you create, including all of the information within your presentations, and your user name will be available to anyone who has access to the internet ("Public User Content"). Public presentations can be viewed by other Prezi users, will appear in the searchable Prezi database, and will be available for others to access and view online. Accordingly, you hereby do and shall grant to each User and to the public a worldwide, non-exclusive, revocable license to access, view and publicly perform your Public User Content. This license ends when you delete the presentation or your account is closed (either by you or by us), except to the extent that the content has been shared with others and they have not deleted it."

In april 2018 had Prezi al meer dan 100 miljoen gebruikers, die bij elkaar al meer dan 325 miljoen openbare presentaties hadden gemaakt. De hoeveelheid gevoelige informatie die daar onbedoeld publiek mee is gemaakt, is niet voor mogelijk te houden en zelfs voor mij, met mijn achtergrond in IT security, schrikbarend te noemen.

De mogelijke gevolgen

Om maar even een open deur in te trappen: je plannen voor het komende jaar online zetten zodat het inzichtelijk is voor al je concurrenten is geen goed idee. Maar ook cijfers, zoals je jaarcijfers, concurrentieonderzoeken, budgetverdelingen en omzet- en winstmarges wil je niet zomaar aan iedereen kunnen uitdelen. Met salarisoverzichten (met of zonder bijbehorende foto en bonusstructuur) heeft een hacker al een mooi startpunt voor een social

Stefanie Weber

Copywriter - Vertaler - Content Creator

engineering aanval, maar vergeet ook gewone phishing aanvallen niet.

En wat te denken van CEO fraude? Administratieve cijfers bieden daar ook de mogelijkheid toe. Vaak staan de presentaties gewoon op naam van een medewerker of stagiair, waardoor hackers ook meteen een ingang hebben om verder te zoeken bij een bedrijf.

Maar daarnaast telt het zelf online zetten van deze gegevens ook gewoon als datalek, die gemeld moet worden bij de Autoriteit Persoonsgegevens (AP). Aan het lekken van gegevens kan tegenwoordig een flinke boete kleven.

Blijf op de hoogte

Het beste advies wat ik kan geven is: lees je in. Zeker bij software die gratis in de cloud, of als gratis proef wordt aangeboden, is het belangrijk om te weten wat er gebeurt met de gegevens en producten die jij maakt met die gratis software. Lees daarom altijd de algemene voorwaarden goed door. Zijn de algemene voorwaarden niet duidelijk genoeg, overweeg dan om een alternatief te gebruiken.

Zorg er daarnaast voor dat je bedrijf gebruik maakt van een duidelijk beleid met betrekking tot het publiceren van gegevens. Hierin kun je opnemen dat er alleen gebruik gemaakt mag worden van cloud applicaties met goede, sterke privacy settings. Zo voorkom je dat er buiten de IT afdeling om applicaties worden geïnstalleerd of gebruikt in de cloud. Leg alle gebruik van software per afdeling vast in een duidelijk dossier om niet voor onaangename verrassingen komen te staan.

Zelfs als de keuze gevallen is op een applicatie met sterke settings en duidelijke rechten, is het alsnog verstandig om verder te kijken. Waar wordt data opgeslagen? Gebruikt het bedrijf een server in de EU, of slaan ze hun data alleen op in de VS? Hoe gaan ze om met het verwerken en verzenden van die data?

Het gebruiken van handige cloud-based software is voor heel veel bedrijven een uitkomst. Nog steeds vereist het inzicht en kennis om deze echt veilig te kunnen gebruiken. Zorg er dus voor dat jouw data echt jouw data blijft.