BEDRIJFSVERTROUWELIJK

RAPPORTAGE CYBER RISICO SCAN

MANAGEMENTRAPPORTAGE

Bouwend Nederland

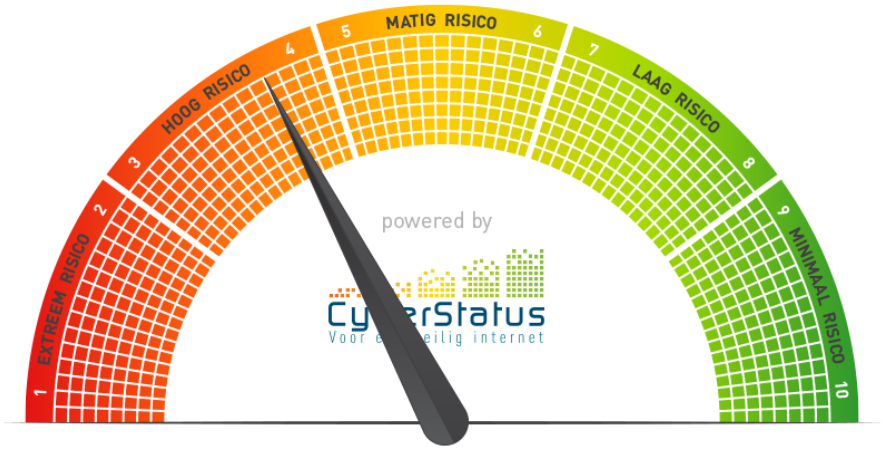
Veilig Online Ondernemen

ALGEMENE INFORMATIE

gescand

Scan op:	Linux-test.threadstone.nl
Datum scan:	30 november 2016

CyberStatus
Voor een veilig internet



HET CIJFER VAN DE CYBER RISICO SCAN IS: 4* (HOOG RISICO)

Uw website of bedrijfsnetwerk is onvoldoende beveiligd tegen cyberinbraken. We hebben kwetsbaarheden ontdekt met een hoge prioriteit: kwaadwillenden kunnen eenvoudig op uw site of bedrijfsnetwerk inbreken. Raadpleeg zo snel mogelijk uw IT-leverancier om het hoge risico op dataverlies te verkleinen.

* Gebaseerd op de score-indeling van ThreadStone

SAMEN STERKER: BETREK UW IT-PARTNER!

- Digitale beveiliging verdient aandacht van u, maar ook van uw IT-partner(s). Spreek dit rapport in een constructief gesprek door en maak duidelijke afspraken naar de toekomst wie-waarvoor verantwoordelijk is.
- Deze rapportage geeft u concrete handvatten om de beveiliging van uw IT-systeem verder te verbeteren. Uw IT-partner kan met de uitkomsten in deze rapportage zien hoe hoog het risico is dat u loopt en waar mogelijke kwetsbaarheden van uw systeem liggen.
- Maak heldere afspraken met uw IT-partner welke maatregelen zullen worden getroffen. In navolgende scans kunt u samen monitoren of deze het gewenste effect hebben.

VEILIGHEIDSTIPS VAN CYBERSTATUS

- Helaas is niemand volledig beschermd, zelfs niet als u een 10 scoort. Geen enkele beveiliging is (continue) 100%.
- Maandelijks worden er gemiddeld 500 nieuwe kwetsbaarheden gevonden. Zorg er dus voor dat u periodiek uw beveiliging controleert. Het CyberStatus platform ondersteund een controle per kwartaal of per half jaar.
- Deze scan geeft een indicatie van uw beveiliging. Voor websites is bijvoorbeeld niet de onderliggende infrastructuur gecontroleerd (alleen poort 80 en 443 worden gecontroleerd) en voor bedrijfsnetwerken worden de eventueel achterliggende webpagina's niet gecontroleerd. Indien u meer uitgebreid wilt controleren, extra IP-adressen wilt toevoegen, vaker wilt controleren of grondiger wilt scannen, neem dan contact op met uw IT-partner en vraag naar de mogelijkheden.
- Vanuit de nieuwe Meldplicht datalekken dient u passende maatregelen te treffen om aan uw ondernemersplicht te voldoen. Boetes kunnen hoog oplopen. Zorg er dus voor dat u duidelijke afspraken maakt; ú bent verantwoordelijk!
- Focus op versterking: deze scan-tool wordt u aangeboden om uw systeem samen met uw IT-partner te verbeteren. Veilig Online Ondernemen heeft u zelf in de hand.
- Maak afspraken met uw partners in de keten. Zorg er voor dat de koppelvlakken waar digitale informatie wordt uitgewisseld tussen partijen ook regelmatig wordt voorzien van een controle op kwetsbaarheden. De keten is zo sterk als de zwakste schakel.
- Deze scan levert inzicht op technisch gebied. Goede beveiliging besteedt ook aandacht aan mensen, beleid en procedures. Neem met uw IT-partner de verschillende opties door.
- Overweeg een Cyber risico verzekering. Neem dit door met uw verzekeringsagent.
- Bereid u voor op een datalek; het kan iedereen overkomen! Zet een incident responseplan op, zodat u weet wat u moet doen als u slachtoffer wordt.
- Zorg er voor dat u een bewuste en goede opdrachtgever richting uw leveranciers bent. Maak duidelijke afspraken over beveiliging en zorg voor zogenaamde bewerkersovereenkomsten als u werkzaamheden uitbesteed aan derden waar persoonsgegevens bij betrokken zijn.

- Binnen de bouw wordt veel gewerkt met grote bestanden (tekeningen) over projecten en producten. Let er op dat deze via een beveiligd medium worden gecommuniceerd. Het uitwisselen via bijvoorbeeld ZIP bestanden kan tot verhoogde risico`s leiden, omdat virussen ook eenvoudig via ZIP bestanden verspreid kunnen worden. Zet hier een apart beleid voor op.
- Projecten en producten zijn over het algemeen de meest belangrijke `assets` van bedrijven in onze sector. Zorg er voor dat bij elk project digitale beveiliging als serieus aandachtspunt wordt meegenomen in de projectbeschrijvingen en opdrachtbevestigingen. Hiermee versterkt u uw eigen positie t.o.v. uw concurrenten, omdat uw klanten steeds meer en meer zullen vragen om zekerheid rond digitale beveiliging. Gebruik digitale beveiliging dus als kans om u te onderscheiden!
- Er wordt veel met onderaannemers gewerkt. Zorg er voor dat u aandacht geeft aan bijvoorbeeld bewerkersovereenkomsten op het moment dat u gegevens uitlevert van uw klanten richting deze onderaannemers. De keten is zo sterk als de zwakste schakel en ook hier geldt dat uw klanten steeds vaker zullen gaan vragen hoe u dit aspect in uw bedrijf heeft geregeld.

Zorg voor periodieke herziening van uw digitale beveiligingsplannen en -beleid. Het is geen `rocket science`, zolang u er bewust mee bezig bent en het periodiek op de management agenda plaatst. Zorg er dus ook voor dat u een plan maakt voor het geval dat. Als u op dat moment alles moet gaan regelen, dan bent u zeker te laat en weet u zeker dat de kosten van een datalek vele malen hoger zullen zijn dan dat u zich hebt voorbereid.

Wij wensen u een succesvolle bouw van uw organisatie toe!

Kwetsbaarheden met kritieke prioriteit:	0
Kwetsbaarheden met hoge prioriteit:	1
Kwetsbaarheden met medium prioriteit:	19
Kwetsbaarheden met lage prioriteit:	4
Informatieve kwetsbaarheden:	38
Scan afgebroken door firewall of Intrusion detection systeem:	NEE

GEVONDEN KWETSBAARHEDEN MET HOGE PRIORITEIT

BESCHRIJVING	CVSS SCORE*	EXPLOIT BESCHIKBAAR*
A CGI application hosted on the remote web server is potentially prone to SQL injection attack.	7,5	-

GEVONDEN KWETSBAARHEDEN MET MEDIUM PRIORITEIT

BESCHRIJVING	CVSS SCORE*	EXPLOIT BESCHIKBAAR*	
The remote web application discloses path information.	5,0	-	
The remote web server might be prone to cross-site request forgery attacks.	6,4	-	
The remote web server contains a PHP application that is affected by an information disclosure vulnerability.	5,0	-	
The remote web server uses a version of PHP that is affected by a security bypass	6,2	Ja	
The remote web server uses a version of PHP that does not properly validate user strings.	5,0	-	
The remote web server uses a version of PHP that is affected by a security bypass	4,3	Ja	
Some directories on the remote web server are browsable. This could be a databreach.	5,0	-	TOP 100
The remote Apache server is vulnerable to multiple privilege escalation attacks.	6,2	Ja	
The remote Apache server is vulnerable to an information disclosure attack.	4,3	Ja	TOP 100
The remote web server is affected by an information disclosure issue.	4,3	Ja	
The configuration of PHP on the remote host allows disclosure of sensitive information.	5,0	-	
Debugging functions are enabled on the remote web server.	5,0	Ja	
The remote web server may fail to mitigate a class of web application vulnerabilities.	4,3	-	

It may be possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.	4,3	Ja
The SSL certificate for this service cannot be trusted.	6,4	-
The SSL certificate chain for this service ends in an unrecognized self-signed certificate.	6,4	-
The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.	-	-
An insecure port, protocol, or service has been detected.	-	-
Remote access software has been detected.	-	-

GEVONDEN KWETSBAARHEDEN MET LAGE PRIORITEIT

BESCHRIJVING	CVSS SCORE*	EXPLOIT BESCHIKBAAR*
The remote web server uses a version of PHP that is affected by a security bypass	3,2	Ja
The remote service supports the use of the RC4 cipher.	2,6	Ja
The remote service supports the use of 64-bit block ciphers.	2,6	Ja
The remote web server might transmit credentials in cleartext.	2,6	-

GEVONDEN INFORMATIEVE KWETSBAARHEDEN

BESCHRIJVING	CVSS SCORE*	EXPLOIT BESCHIKBAAR*
Security patches are backported.	-	-
Security patches have been backported.	-	-
It is possible to obtain the version number of the remote PHP install.	-	-
The remote web server is not enforcing HSTS.	-	-
An application was found that may use CGI parameters to control sensitive information.	-	-
The remote web server hosts a database management application written in PHP.	-	-
This plugin determines which HTTP methods are allowed on various CGI directories.	-	-
The version of OpenSSL can be identified.	-	-
Some information about the remote HTTP configuration can be extracted.	-	-
The remote web server contains a blog application written in PHP.	-	-

A web server is running on the remote host.	-	-
The remote web server hosts linkable content that can be crawled by our scanners.	-	-
HTTP session cookies might be transmitted in cleartext.	-	-
Email addresses were harvested from the web server.	-	-
The remote web server does not take steps to mitigate a class of web application	-	-
The remote web server does not take steps to mitigate a class of web application	-	-
HTTP session cookies might be vulnerable to cross-site scripting attacks.	-	-
The 'autocomplete' attribute is not disabled on password fields.	-	-
Links to external sites were gathered.	-	-
Our scanner can crawl the remote website.	-	-
It is possible to enumerate directories on the web server.	-	-
The remote host allows resuming SSL sessions.	-	-
The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.	-	-
The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.	-	-
The remote service encrypts communications using SSL.	-	-
A root Certification Authority certificate was found at the top of the certificate chain.	-	-
This plugin displays the SSL certificate.	-	-
The remote service encrypts communications.	-	-
It is possible to determine which TCP ports are open.	-	-
It was possible to obtain traceroute information.	-	-
It is possible to enumerate CPE names that matched on the remote system.	-	-
It is possible to guess the remote device type.	-	-
It is possible to guess the remote operating system.	-	-
The name of the Linux distribution running on the remote host was found in the banner of the web server.	-	-
This plugin detects the protocols understood by the remote IP stack.	-	-
The remote service implements TCP timestamps.	-	-

It was possible to resolve the name of the remote host.	-	-
It is possible to determine the exact time set on the remote host.	-	-

* voor nadere uitleg over de CVSS score en de betekenis van exploits verwijzen we naar hoofdstuk "Score kwetsbaarheden conform CVSS"

We hebben onderzoek gedaan naar de top-100 kwetsbaarheden die in onze systemen voorkomen op basis van de scans die in het verleden zijn uitgevoerd. Voor deze top-100 hebben we geprobeerd om in begrijpelijke taal te beschrijven wat het probleem exact inhoudt en wat de impact kan zijn op het moment dat misbruik zou worden gemaakt van de kwetsbaarheid. In dit hoofdstuk wordt dit per gevonden kwetsbaarheid beschreven.

Let op! Aangezien deze gegevens uit onze top-100 komt, zal deze lijst waarschijnlijk niet compleet zijn. Voor kwetsbaarheden die als "informatief" zijn geclassificeerd zal bijvoorbeeld geen mogelijke business impact zijn beschreven. Richt u dus niet alleen op deze beschrijvingen, maar neem alle geconstateerde problemen door met uw IT-leverancier!

Some directories on the remote web server are browsable. This could be a databreach.

MOGELIJKE BUSINESS IMPACT
Er zijn mappen en bestanden gevonden op uw website die vrij te benaderen zijn. Het kan zijn dat deze bestanden bewust benaderbaar zijn gemaakt, maar het kan ook zijn dat deze bestanden gevoelige data bevatten.

ADVIES
Laat controleren welke bestanden vanaf het internet benaderbaar zijn en verzeker uzelf dat zich hierin geen gevoelige data bevinden die een datalek kunnen veroorzaken.

The remote Apache server is vulnerable to an information disclosure attack.

MOGELIJKE BUSINESS IMPACT
Het lijkt er op dat de code van de webpagina eenvoudig opvraagbaar is.

ADVIES
Controleer bijvoorbeeld de opvraag van een PHP pagina, gevolgd door een backslash. Het kan zijn dat de broncode wordt weergegeven in plaats van dat de code wordt uitgevoerd.

The version of OpenSSL can be identified.

MOGELIJKE BUSINESS IMPACT
De gebruikte versie van OpenSSL kan worden achterhaald. Hierdoor kan - bij achterstallig onderhoud - gezien worden dat er bijvoorbeeld een oude versie van OpenSSL wordt gebruikt.

ADVIES
Laat controleren of deze setting kan worden dichtgezet of zorg ervoor dat in ieder geval het patch-level van OpenSSL niet wordt getoond. Hierdoor is er minder informatie beschikbaar voor kwaadwillenden.

The remote web server hosts linkable content that can be crawled by our scanners.

MOGELIJKE BUSINESS IMPACT
De server bevat content met links die gebruikt kunnen worden om meer informatie te achterhalen.

ADVIES
Zorg voor zgn. hardening van de server en zorg er voor dat er minimale informatie naar buiten wordt afgegeven, zodat kwaadwillenden ook zo min mogelijk informatie kunnen achterhalen. Alle informatie die getoond wordt kan - nu of in de toekomst - een mogelijk datalek veroorzaken.

Our scanner can crawl the remote website.

MOGELIJKE BUSINESS IMPACT
Er kan een kopie worden gemaakt van de website en vervolgens kan een lijst worden opgevraagd van de zgn. CGI-scripts die op de server draaien. Deze informatie hoeft niet beschikbaar te zijn.

ADVIES
Laat het aantal pagina's dat gespiegeld kan worden aanpassen.

OVER DIT RAPPORT (WARRANTY AND WAIVER)

Dit rapport bevat uitkomsten over de Cyber Risico Scan die is verricht door ThreadStone Cyber Security B.V. (hierna: "ThreadStone"). De vrijwaringsverklaring, gebruikersvoorwaarden, privacy verklaring, bewerkersovereenkomst en disclaimer - zoals te vinden op onze internetsite www.cyberstatus.nl - zijn te allen tijde van toepassing op dit rapport.

De scan scant alleen op kwetsbaarheden die vanaf het externe netwerk zichtbaar zijn (een zgn. outside-in scan). Dit betekent dat het rapport alleen kwetsbaarheden opsomt die vanaf het internet detecteerbaar zijn. De scans worden uitgevoerd op een veilige manier; dit betekent dat (Distributed) Denial of service-aanvallen ((D)DoS-aanvallen) niet in de scan worden uitgevoerd.

ThreadStone voert de scans uit vanaf een serverpark in Duitsland en Nederland. De scans zijn uitgevoerd vanuit de IP adressen 78.46.19.149 en 5.9.17.13. Zorg er voor dat deze IP nummers op de "allow" list staan van uw firewalls.

Indien u een firewall gebruikt die alle contactpogingen in logbestanden plaatst, dan zullen de scans vanaf onze IP-adressen in de logs terugkomen. De logmeldingen waarin onze IP adressen zijn genoemd zijn afkomstig van de servers van ThreadStone Cyber Security en zijn op geen enkele wijze een poging tot inbraak of poging tot toebrengen van schade. U kunt de logbestanden zien als handige informatie dat uw detectiesystemen juist functioneren.

ThreadStone is een Cyber Security bedrijf dat veiligheid scans (vulnerability scans) en penetratie testen uitvoert. ThreadStone heeft certificeringen als EC Council Licenced penetratie tester, Certified Ethical hacker en Certified security analyst. De scans worden met de grootste zorg en uiterste precisie uitgevoerd. Wij kunnen echter geen garanties geven voor wat betreft de inhoud of volledigheid van dit rapport.

CyberStatus, ThreadScan en ThreadStone zijn een handelsmerk van ThreadStone Cyber Security B.V.. Alle andere product- en bedrijfsnamen zijn handelsmerken of geregistreerde handelsmerken van andere partijen.

Met dit verslag wordt u mogelijk verwezen naar andere websites, rapporten en technische oplossingen die niet onder de controle staan van ThreadStone. Wij hebben daarom geen controle over de aard, inhoud en de beschikbaarheid van deze bronnen. Daarnaast zijn deze bronnen aan tussentijdse verandering onderhevig, waardoor bepaalde informatie mogelijk niet meer actueel en compleet kan zijn. De opname van welke informatie dan ook is niet noodzakelijkerwijs een aanbeveling of onderschrijving van standpunten die door andere bronnen worden geuit en hebben slechts een informatieve strekking.

Uitleg betekenis CVSS score

De geconstateerde kwetsbaarheden worden gekwalificeerd conform de score van CVSS. Dit is een vrije en open industriestandaard voor de beoordeling van de ernst van kwetsbaarheden in computersystemen en websites. De standaard is onder beheer van het Forum of Incident Response and Security Teams (FIRST).

CVSS kwalificeert kwetsbaarheden op risico in vergelijking met andere kwetsbaarheden, zodat benodigde inspanningen vervolgens kunnen worden geprioriteerd. De scores zijn gebaseerd op een aantal metingen (metriek genoemd) op basis van evaluatie door deskundigen. De scores lopen van 0 tot 10. Beveiligingsproblemen met een basisscore in het bereik 9.0-10.0 zijn kritisch, die in het bereik 7.0-8,9 zijn hoog, 4.0-6,9 zijn medium en 0.1-3.9 zijn laag.

Voor de volledigheid worden ook de informatieve berichten (score 0) geregistreerd en gerapporteerd.

De Cyber Risico Scan vertaalt de CVSS score automatisch naar een eigen score, gebaseerd op de kwetsbaarheid met de hoogste score op CVSS.

Score conform CVSS

Critical	9.0..10.0
High	7.0..8.9
Medium	4.0..6.9
Low	0.1..3.9
Information	0

Uitleg betekenis ‘Exploit beschikbaar’

Met behulp van een exploit kan een kwaadwillend persoon misbruik maken van een kwetsbaarheid in uw website of bedrijfsnetwerk. Een exploit is een klein programma waarmee iemand via een kwetsbaarheid bijvoorbeeld toegang kan krijgen tot uw systeem. Exploits voor bekende kwetsbaarheden zijn soms ook makkelijk te vinden op het internet. In het overzicht van gevonden kwetsbaarheden wordt per kwetsbaarheid aangegeven of er exploits bekend zijn. Dit betekent niet direct dat uw website of bedrijfsnetwerk reeds misbruikt is; het geeft aan dat uw website of bedrijfsnetwerk - over het algemeen - relatief eenvoudig misbruikt kán worden.

Wat geeft mijn score aan?

De kwetsbaarheden worden geprioriteerd conform de internationale open industrie standaard: CVSS. De CVSS-score geeft een onafhankelijke weging aan een kwetsbaarheid op basis waarvan de kwetsbaarheden worden gewogen. De getoonde rapportcijfers zijn afgeleid van de CVSS-score op basis van onderstaande tabel.

Let op: Werken aan uw digitale veiligheid is nooit klaar. Zelfs als u een 10 scoort bent u niet 100% veilig. Hackers vinden namelijk steeds nieuwe manieren om uw beveiliging te doorbreken. U zal dus voortduren moeten blijven investeren in uw veiligheid.

SCORE 1-2 Extreem risico

(Urgente actie door IT-leverancier vereist)

Uw website of bedrijfsnetwerk staat open voor cyberinbraken. We hebben kwetsbaarheden ontdekt met een kritische urgentie: kwaadwillenden kunnen zeer eenvoudig op uw site of bedrijfsnetwerk inbreken. Raadpleeg direct uw IT-leverancier om passende maatregelen te treffen en het extreme risico op dataverlies te verkleinen.

SCORE 3-4 Hoog risico

(Directe actie door IT-leverancier vereist)

Uw website of bedrijfsnetwerk is onvoldoende beveiligd tegen cyberinbraken. We hebben kwetsbaarheden ontdekt met een hoge prioriteit: kwaadwillenden kunnen eenvoudig op uw site of bedrijfsnetwerk inbreken. Raadpleeg zo snel mogelijk uw IT-leverancier om het hoge risico op dataverlies te verkleinen.

SCORE 5-6 Matig risico

(Actie door IT-leverancier nodig)

Uw website of bedrijfsnetwerk is redelijk beveiligd tegen cyberinbraken, maar er zijn kwetsbaarheden gedetecteerd. Hierdoor is er sprake van een gematigd risico, wat betekent dat kwaadwillenden redelijk eenvoudig digitaal kunnen inbreken. Raadpleeg uw IT-leverancier om deze kwestbaarheiden weg te nemen en het risico op dataverlies te verkleinen.

SCORE 7-8 Laag risico

(Actie door IT leverancier gewenst)

Uw website of bedrijfsnetwerk is goed beveiligd tegen cyberinbraken, maar er zijn wel kwetsbaarheden ontdekt waardoor kwaadwillenden kunnen inbreken. Hiervoor moeten zij redelijk wat moeite doen. Raadpleeg uw IT-leverancier hoe deze kwetsbaarheden kunnen worden weggenomen om het risico op dataverlies te verkleinen.

SCORE 9-10 Erg laag risico

(Geen directe actie nodig)

Uw website of bedrijfsnetwerk is zeer goed beveiligd tegen cyberinbraken. Er zijn op dit moment geen of vrijwel geen kwetsbaarheden ontdekt waardoor kwaadwillenden kunnen inbreken.

CVSS score	Mogelijkheid van misbruik bekend (exploit)?	Score ThreadStone	Kwalificatie ThreadStone
Critical	Ja	1	Extreem risico
	Nee	2	
High	Ja	3	Hoog risico
	Nee	4	
Medium	Ja	5	Matig risico
	Nee	6	
Low	Ja	7	Laag risico
	Nee	8	
Information	Ja	9	Erg laag risico
	Nee	10	