

WHITEPAPER

TOP 10 MEEST VOORKOMENDE CYBER KWETSBAARHEDEN BIJ NEDERLANDSE GEMEENTEN

OP BASIS VAN MEER DAN 600 SUCCESVOL UITGEVOERDE PENTESTEN

PRIVACY STATEMENT

Dit document is eigendom van NFIR. Het mag niet worden gereproduceerd of gebruikt in andere rapporten of publicaties zonder expliciete schriftelijke toestemming van NFIR. Voor vragen of verzoeken om toestemming, neem contact op met NFIR.

DOELEINDEN

De besproken kwetsbaarheden worden wereldwijd misbruikt, zo ook bij de Nederlandse gemeenten. Het doel van deze paper is gemeenten inzicht te geven in huidige dreigingen en hen te helpen bij het verbeteren van beveiligingsmaatregelen. NFIR streeft naar transparantie om de weerbaarheid van gemeenten te verhogen en cyberaanvallen proactief tegen te gaan.

CONTACT

NFIR B.V.

 info@nfir.nl

 +31 (0)88 323 0205

 Kantoor Rijswijk, Laan van Zuid Hoorn 165, Rijswijk

 Kantoor Zwolle, Burgermeester Roelenweg 12, Zwolle

Voorwoord

Gemeenten vormen een essentieel onderdeel van onze samenleving en beheren veel gevoelige gegevens. Toch blijkt uit de praktijk dat bepaalde type kwetsbaarheden veelvuldig voorkomen. Door deze whitepaper te delen willen we **bewustwording** creëren en gemeenten helpen om hun digitale weerbaarheid structureel te verbeteren.

Hoe willen wij bewustwording creëren?

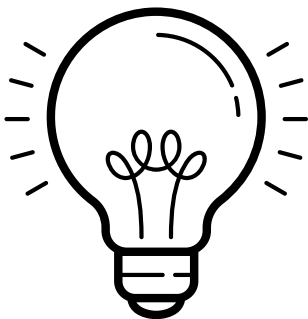
Dit document biedt een overzicht van de meest voorkomende kwetsbaarheden binnen Nederlandse gemeenten. De bevindingen zijn gebaseerd op de kwetsbaarheden die de ethisch hackers van NFIR het vaakst tegenkomen. Het benadrukt de noodzaak van proactieve cyberbeveiliging en beleid door bestuurders van gemeenten.

De whitepaper

In deze whitepaper wordt per kwetsbaarheid aangetoond waar het vaak misgaat en waarom deze kwetsbaarheden flinke impact kunnen hebben. Geschreven vanuit de praktijk, zodat u er vandaag nog iets mee kunt.

Over NFIR

NFIR is een toonaangevend expert op het gebied van cybersecurity en helpt al jarenlang meerdere gemeenten in Nederland hun digitale weerbaarheid te versterken. Als specialist in het voorkomen, opsporen en bestrijden van cyberdreigingen biedt NFIR verschillende diensten aan, zoals pentesten, security monitoring, Incident Response en Digitaal Forensisch Onderzoek.



In 2023 ontvingen Nederlandse gemeenten 141 meldingen van cyberaanvallen, een aanzienlijke stijging ten opzichte van 58 meldingen in 2022.*



Van de meer dan 10.000 gemeentelijke websites voldoet slechts 28% aan de verplichte beveiligingsstandaarden, zoals veilige e-mailconfiguratie en HTTPS-verbindingen.*



Het Cybersecuritybeeld Nederland 2024 meldt een intensivering van activiteiten en verbreding van capaciteiten van statelijke actoren.

* AG connect, 10 april 2024
* Samen Digitaal Veilig, 2024

De Pentest

Een penetratietest, vaak afgekort als pentest, is een doelbewuste en gecontroleerde simulatie van een cyberaanval op een IT-systeem, netwerk, API, OT of (web)applicatie. Het doel van deze test is om kwetsbaarheden en zwakke plekken in de beveiliging op te sporen voordat kwaadwillende hackers dat kunnen doen. Ethische hackers gebruiken dezelfde technieken en strategieën die 'kwaadwillende' aanvallers hanteren, maar doen dat zonder de intentie om schade aan te richten. Een pentest helpt organisaties om potentiële risico's te identificeren en om beveiligingsmaatregelen te verbeteren zodat de kans op een succesvolle aanval aanzienlijk wordt verkleind. Het is een essentieel onderdeel van een bredere beveiligingsstrategie om de integriteit en veiligheid van IT-systemen te waarborgen.

Black, grey & whitebox pentest aanvalsscenario's

Pentesten komen in 3 verschillende aanvalsscenario's, de Blackbox, Greybox en Whitebox aanvalsscenario's. Hieronder volgt een korte introductie tot de 3 aanvalsscenario's.

Bij een Black Box aanvalsscenario wordt vooraf minimale informatie verstrekt door de opdrachtgever. De ethische hackers zullen als 'buitenstaanders' opereren zonder voorkennis. De pentesters gebruiken diverse technieken, waaronder Open Source Intelligence (OSINT) om informatie te vergaren en zwakke plekken te ontdekken.

Bij een White Box aanvalsscenario (ook wel Crystal box genoemd), wordt vooraf alle informatie verstrekt om gericht op zoek te gaan naar kwetsbaarheden. Aanvullend hierop wordt gebruik gemaakt van broncode, logbestanden en toegang tot de server. Daarnaast kan er gebruik gemaakt van de mogelijkheid om een eigen testomgeving op te zetten.

Een Grey Box aanvalsscenario zit tussen een Black en White box in. Er wordt 'beperkt' informatie gedeeld die gebruikt wordt om een omgeving te onderzoeken. De ethisch hackers zullen veelal gebruik maken van een gebruikersaccount voor het onderzoek.

CCV-kwaliteitskeurmerk pentesten

Het CCV pentest keurmerk gaat vooral over de gehanteerde processen en certificeringen van pentesters. De uitvoering van een pentest moet deskundig plaatsvinden. De certificering van een pentest met het CCV-keurmerk Pentesten borgt de kwaliteit van de pentesten en zorgt ervoor dat afnemers van de pentesten van NFIR een gerechtvaardigd vertrouwen kunnen hebben dat de geleverde pentest voldoet aan de vooraf gestelde eisen.



A vertical blue gradient bar on the left side of the page, transitioning from a darker blue at the top to a lighter blue at the bottom.

TOP 10 MEEST VOORKOMENDE CYBER KWETSBAARHEDEN BIJ GEMEENTEN

10

WI-FI KWETSBAARHEDEN

Oorzaken

Veel organisaties maken gebruik van Wi-Fi (WPA Enterprise) met persoonlijke logins. Daarbij wordt meestal gewerkt met een gebruikersnaam en wachtwoord, en niet met een certificaat. Deze wachtwoorden zijn vaak gekoppeld aan de Active Directory.

Gevaren

Een aanvaller kan een rogue access point (een 'neppe' access point die doet alsof deze legitiem is) opzetten om inloggegevens te onderscheppen. Vooral oudere apparaten sturen wachtwoorden soms in leesbare tekst of als zwakke hashes. Omdat de inlog gekoppeld is aan de Active Directory, kan een aanvaller na onderschepping eenvoudig verdere toegang tot de infrastructuur en applicaties krijgen.

Advies

Stap over op een Wi-Fi oplossing in combinatie met persoonlijke certificaten. Door deze certificaten geautomatiseerd te installeren op laptops en smartphones wordt het risico op onderschepping en misbruik aanzienlijk verkleind.

9

BEHEERPORTALEN BESCHIKBAAR

Oorzaken

Beheerportalen, zoals die van firewalls, zijn soms direct via het internet toegankelijk. Ook worden bepaalde poorten van systemen of applicaties opengezet, waardoor deze publiek beschikbaar zijn.

Gevaren

Beheerportalen van firewallleveranciers bevatten regelmatig kwetsbaarheden. Wanneer een geopende poort kwetsbaar blijkt kunnen aanvallers dit misbruiken om toegang te krijgen tot het interne netwerk.

Advies

Zorg dat beheerportalen nooit direct vanaf het internet bereikbaar zijn, maar plaats ze achter een VPN. Beperk daarnaast het aantal extern toegankelijke poorten zoveel mogelijk om het aanvalsoppervlak te verkleinen.

8

NETWERK- SEGMENTATIE ONVOLDOENDE TOEGEPAST

Oorzaken

Binnen veel interne infrastructuren wordt netwerksegmentatie toegepast met verschillende VLAN's, maar al het verkeer tussen deze VLAN's wordt geregeld toegestaan. Vaak is er geen firewall tussen de segmenten. Daarnaast wordt netwerkaccess control (NAC) niet geïmplementeerd.

Gevaren

Wanneer een kwaadwillende toegang krijgt tot één systeem of netwerksegment, kan hij zich eenvoudig verspreiden over het gehele netwerk. Door simpelweg een netwerkkabel in te pluggen op uw locatie, kan direct toegang worden verkregen tot het netwerk.

Advies

Beperk het verkeer tussen verschillende netwerksegmenten en blokkeer standaard al het verkeer tussen VLAN's, tenzij er specifieke regels zijn opgesteld. Pas microsegmentatie toe zodat servers geen volledige toegang hebben tot andere servers. Implementeer netwerkaccess control (NAC) op basis van certificaten en het 802.1x-protocol en zorg ervoor dat toegang niet wordt verleend op basis van MAC-adressen. Beperk ook de poorten die toegang geven tot het internet.

7

GEEN OF BEPERKTE SECURITY MONITORING

Oorzaken

Veel gemeenten gebruiken geen of een beperkte MDR (Managed Detection and Response) of SOC (Security Operations Center) dienst. Daarnaast biedt anti-virus of endpoint protection software vaak onvoldoende detectiecapaciteit. In sommige gevallen kan deze software zelfs worden uitgeschakeld of is het mogelijk om uitzonderingen toe te voegen.

Gevaren

Zonder een security monitoring dienst is er geen zicht op dreigingen binnen de infrastructuur. Een aanvaller die toegang krijgt tot een systeem kan de AV-software uitschakelen en verder toegang verkrijgen tot het netwerk. Dit stelt de aanvaller in staat om dumps te maken van Windows-systemen, wat kan leiden tot het verkrijgen van gebruikers- of beheerdersaccounts.

Advies

Implementeer security monitoring om real-time inzicht te krijgen in je netwerk en om snel in te grijpen bij dreigingen. Maak gebruik van anti-virus en endpoint protection software die niet lokaal uitgeschakeld kan worden en die geen uitzonderingen toestaat. Zorg ervoor dat deze software op alle systemen geïnstalleerd is.



6

TOEGANG TOT GEVOELIGE DATA OP FILESHARES

Oorzaken

Binnen veel gemeenten hebben gebruikers automatisch toegang tot fileshares die hen 'teveel' rechten geven. Dit gebeurt vaak zonder onderscheid te maken, waardoor gevoelige informatie voor een groot aantal mensen toegankelijk is. Daarnaast worden oude bestanden die niet meer nodig zijn niet opgeruimd. Hierdoor blijven ze voor iedereen beschikbaar.

Gevaren

Deze situatie biedt aanzienlijke risico's voor de organisatie. Gevoelige gegevens die voor iedereen toegankelijk zijn kunnen door een aanvaller worden misbruikt om verder toegang te verkrijgen tot het netwerk. Als een aanvaller toegang heeft tot deze gegevens kan hij de vertrouwelijke informatie gebruiken voor schadelijke doeleinden. Het risico op datalekken is aanzienlijk, aangezien alle gegevens inclusief persoonsgegevens en vertrouwelijke bedrijfsinformatie voor onbevoegden beschikbaar zijn. Het gevaar wordt verder vergroot wanneer volledige systeemback-ups beschikbaar zijn. Als een aanvaller toegang heeft tot deze back-ups, kan hij ze openen en gebruiken om toegang te krijgen tot systemen, wat ernstige schade kan veroorzaken.

Advies

Om deze risico's te minimaliseren is het van cruciaal belang om ervoor te zorgen dat fileshares alleen toegankelijk zijn voor de gebruikers die deze daadwerkelijk nodig hebben om hun werk uit te voeren. Dit vereist een regelmatige inventarisatie van de beschikbare fileshares en de toegang die gebruikers hebben. Daarnaast moeten bestanden die niet meer nodig zijn periodiek worden verwijderd of gearchiveerd om te voorkomen dat verouderde informatie onterecht beschikbaar blijft.

5

GEEN OF BEPERKT ASSET BEHEER

Oorzaken

Een veelvoorkomende oorzaak van beveiligingsrisico's binnen organisaties is het gebruik van verouderde software en besturingssystemen. Veel systemen draaien op softwareversies die niet meer worden ondersteund of ontvangen geen beveiligingsupdates meer. Dit maakt ze kwetsbaar voor aanvallen. Daarnaast is er vaak geen volledig inzicht in welke systemen er binnen de gemeente aanwezig zijn en waarvoor deze gebruikt worden. Dit zorgt ervoor dat verouderde of niet-gebruikte systemen onopgemerkt blijven. Het komt ook voor dat oude systemen niet op tijd worden uitgeschakeld of opgeruimd, ondanks dat medewerkers vaak aangeven dat deze systemen al lange tijd niet meer in gebruik zijn of dat ze nog opgeruimd moeten worden.

Gevaren

Het gebruik van verouderde software brengt aanzienlijke risico's met zich mee. Deze software heeft vaak bekende beveiligingslekken die door aanvallers kunnen worden misbruikt om toegang te krijgen tot het systeem of zelfs volledige controle over te nemen. Verouderde besturingssystemen ontvangen geen regelmatige beveiligingspatches, waardoor ze een aantrekkelijk doelwit zijn voor cybercriminelen.

Door deze systemen blijven kwetsbaarheden bestaan die eenvoudig kunnen worden geëxploiteerd, wat kan leiden tot datalekken, systeemcompromis of zelfs een volledige netwerkcompromittering.

5

GEEN OF BEPERKTE ASSET BEHEER

Advies

Om de risico's van verouderde software te minimaliseren is het belangrijk om een beleid te implementeren waarin software periodiek wordt bijgewerkt en geüpgraded. Idealiter zou dit proces geautomatiseerd worden om te zorgen voor snelle en betrouwbare updates.

Het is ook cruciaal om inzicht te hebben in welke systemen binnen de organisatie aanwezig zijn, welke software erop draait en wat de rol van deze systemen is binnen de infrastructuur. Dit zorgt ervoor dat er geen ongebruikte of kwetsbare systemen overblijven.

Oude systemen of software die niet meer nodig zijn moeten onmiddellijk worden uitgeschakeld of verwijderd. Indien het onmogelijk is om een verouderd systeem uit te schakelen, moet het geïsoleerd worden van het netwerk om te voorkomen dat aanvallers er toegang toe krijgen.

4

MAN-IN-THE-MIDDLE AANVALLEN

Oorzaken

Onveilige configuraties op protocolniveau kunnen grote risico's met zich meebrengen. Bijvoorbeeld wanneer RDP geen Network Level Authentication (NLA) heeft, kan dit een aanvaller in staat stellen om ongeautoriseerde toegang te verkrijgen. Het niet inschakelen van SMB-signing maakt communicatie tussen systemen kwetsbaar voor man-in-the-middle aanvallen. Het gebruik van onversleutelde protocollen verhoogt de kans op afluisteren van gevoelige gegevens. Ook het inschakelen van het LLMNR-protocol vergroot de kans op naamresolutie-aanvallen. Ten slotte kan het inschakelen van IPv6 zonder daadwerkelijk gebruik ervan zorgen voor onbedoelde kwetsbaarheden in het netwerk.

Gevaren

Een aanvaller kan eerst verhoogde toegang krijgen tot bepaalde accounts. Vanuit die positie kan hij zich verder binnen de organisatie bewegen en steeds meer gevoelige informatie compromitteren. Uiteindelijk kan dit leiden tot Domain Admin toegang, waarmee hij volledige controle over het netwerk heeft en alle data en systemen in gevaar brengt.

Advies

Het is belangrijk om regelmatig een pentest uit te voeren, waarbij specifiek wordt getest op zwakheden binnen de Active Directory en het misbruik hiervan. Gebruikersaccounts moeten alleen de rechten krijgen die strikt noodzakelijk zijn.

3

ACTIVEDIRECTORY KWETSBAARHEDEN

Oorzaken

Foutieve permissies en rechten zijn vaak de oorzaak van beveiligingslekken binnen Active Directory. Bekende kwetsbaarheden zoals Kerberoasting, AS-REP roasting en GPP kunnen door aanvallers worden misbruikt om toegang te krijgen tot gevoelige informatie. Daarnaast worden wachtwoorden soms opgeslagen in omschrijvingen, wat een makkelijke ingang biedt voor aanvallers.

Gevaren

Een aanvaller kan eerst verhoogde toegang krijgen tot bepaalde accounts. Daarmee kan hij steeds dieper in de organisatie doordringen en gevoelige informatie compromitteren. Uiteindelijk kan dit leiden tot Domain Admin toegang, waarmee hij volledige controle over het netwerk krijgt en alle data en systemen in gevaar brengt.

Advies

Het is belangrijk om regelmatig een pentest uit te voeren, waarbij specifiek wordt getest op zwakheden binnen de Active Directory en het misbruik hiervan. Gebruikersaccounts moeten alleen de rechten krijgen die strikt noodzakelijk zijn. Bijvoorbeeld, een serviceaccount heeft alleen toegang nodig tot de specifieke service, en een databasebeheerder heeft enkel rechten op de database servers. Het gebruik van de 'Domain Admin' groep moet worden beperkt. Waar mogelijk moeten deze rechten tijdelijk worden gegeven en na een bepaalde tijd automatisch worden ingetrokken. Daarnaast is het belangrijk om te controleren wanneer accounts voor het laatst zijn gebruikt en oude accounts te verwijderen.

2

ADCS KWETSBAARHEDEN

Oorzaken

Binnen de Active Directory Certificate Server (ADCS) komen vaak foutieve permissies voor. Onjuiste instellingen in certificaattemplates kunnen ervoor zorgen dat aanvallers misbruik maken van de infrastructuur. Verouderde certificaattemplates vormen een extra risico, omdat ze vaak niet voldoen aan moderne beveiligingsstandaarden. Daarnaast staat web enrollment soms ingeschakeld, wat een aanvaller de mogelijkheid geeft om certificaten aan te vragen en zich als legitieme gebruiker voor te doen.

Gevaren

Een aanvaller kan configuratiefouten op templates of op het niveau van de Certificate Authority (CA) gebruiken om een certificaat aan te vragen namens een andere gebruiker. Door dit te doen, kan de aanvaller zich voordoen als een legitieme gebruiker en zelfs Domain Admin-rechten verkrijgen.

Advies

Om de beveiliging te verbeteren, is het belangrijk om templates met foutieve permissies of instellingen te herconfigureren. Verouderde templates moeten worden uitgeschakeld en uiteindelijk verwijderd zodat ze geen risico meer vormen.

1

WACHTWOORDBELEID

Oorzaken

Een veelvoorkomende oorzaak van beveiligingsrisico's binnen gemeenten is het gebruik van zwakke wachtwoorden. Uit eigen ervaring blijkt dat gemiddeld 40% van de accounts een wachtwoord heeft dat eenvoudig te raden of te kraken is. Daarnaast wordt hetzelfde wachtwoord vaak hergebruikt op meerdere systemen, waardoor een inbreuk op één account direct andere systemen in gevaar brengt.

'Standaardwachtwoorden' die in gebruik blijven op systemen geven een makkelijke ingang voor kwaadwillende.

Tot slot wordt Multi-Factor Authenticatie (MFA) niet altijd consequent toegepast.

Gevaren

Wanneer een aanvaller eenmaal toegang krijgt tot een systeem met verhoogde rechten kan deze zich vaak eenvoudig verplaatsen naar andere systemen binnen hetzelfde netwerk (lateral movement).

Daarnaast worden vaak wachtwoorden opgeslagen op onbelangrijke apparaten, zoals printers, die via het netwerk kunnen worden aangesproken. Deze apparaten hebben vaak te veel rechten en bieden een makkelijke toegangspoort voor aanvallers.

Het ontbreken van MFA op interne systemen maakt het mogelijk om in te loggen op accounts zonder extra verificatie. Als een aanvaller eenmaal binnen is kan deze eenvoudig andere accounts compromitteren en toegang krijgen tot gevoelige informatie, wat de schade vergroot.

1

WACHTWOORDBELEID

Advies

Het gebruik van lange, complexe wachtwoorden is essentieel om de kans op een succesvolle aanval te verkleinen. Een minimaal aantal van 12 karakters wordt aanbevolen.

Daarnaast moeten er **geen** uitzonderingen worden gemaakt op het gebruik van MFA; dit zou op alle accounts en systemen verplicht moeten worden gesteld om de beveiliging te versterken.

Het gebruik van een wachtwoordmanager is een uitstekende manier om wachtwoorden veilig op te slaan en te genereren. Dit helpt niet alleen om wachtwoorden uniek te maken voor verschillende websites en diensten, maar zorgt er ook voor dat wachtwoorden moeilijk te raden zijn.

Waar mogelijk maak gebruik van passkeys in combinatie met hardware sleutels of een wachtwoordmanager voor extra beveiliging.

Alle systemen zouden een uniek, automatisch gegenereerd wachtwoord moeten hebben dat door de wachtwoordmanager wordt beheerd, om te voorkomen dat zwakke of gestandaardiseerde wachtwoorden in omloop zijn.

Nawoord

Cybersecurity is geen eenmalige actie, maar een continu proces van bewustwording, verbetering en aanpassing.

”

In deze whitepaper hebben we enkele veelvoorkomende kwetsbaarheden en bijbehorende risico's uitgelicht die wij tijdens onze penetratietesten regelmatig aantreffen. De voorbeelden onderstrepen hoe relatief eenvoudige aanpassingen al een groot verschil kunnen maken in het weerbaarder maken van je gemeente.

”

- Paul Luijben, Teamlead Pentesting NFIR

”

Een aanvaller hoeft maar één fout te vinden. Onze taak is om die fouten vóór hen te vinden en gemeenten bewust te maken van hoe eenvoudig dat soms kan zijn.

”

- Bert Alting, Technical Lead Pentesting NFIR

We hopen dat deze inzichten bijdragen aan het verbeteren van uw IT-beveiliging. Heeft u vragen over de inhoud van deze whitepaper of bent u benieuwd hoe uw gemeente er op dit moment voor staat?

Neem gerust contact met ons op. Of vraag een vrijblijvende offerte aan op onze NFIR pentest webpagina.

We denken graag mee.

