Auditdienst Rijk
Ministerie van Financiën

departementaal VERTROUWELIJK

Onderzoeksrapport

Onderzoeksrapport beveiligingsonderzoek SBP infrastructuur en IRC/LEDA applicatie

Colofon

Titel	Onderzoeksrapport beveiligingsonderzoek SBP infrastructuur en IRC/LEDA applicatie
Uitgebracht aan	Hoofd Eenheid Informatisering Afdelingshoofd RHB
Datum	25 november 2020
Kenmerk	

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding

Het ministerie van Financiën is bezig met een traject om haar ICT dienstverlening die nu nog door de eigen afdeling IT-specials wordt geleverd te outsourcen naar Schuberg Philis (hierna SBP). Op maandag 12 februari 2018 is het contract voor het uitbesteden van ICT dienstverlening van IT Specials getekend met SBP. In mei 2018 is daarna gestart met de bouw van de omgeving. Daarna worden op een gefaseerde wijze onderdelen van de dienstverlening bij de leverancier ondergebracht. De verwachting bij de start van dit onderzoek was dat dit nog tot halverwege 2019 zou duren.

In het kader van de transitie van de IT-omgeving naar SBP is binnen het daartoe opgetuigde project ook vastgelegd dat er een beveiligingsonderzoek (pentest) op de nieuwe omgeving bij SBP, inclusief de IRC/LEDA applicatie van de Rijkshoofdboekhouding (RHB), dient te worden uitgevoerd door een onafhankelijke partij.

Op basis van bovenstaande heeft het Ministerie van Financiën de ADR gevraagd het betreffende beveiligingsonderzoek, inclusief hertest, uit te voeren.

1 Managementsamenvatting

In deze managementsamenvatting kunt u de belangrijkste bevindingen lezen uit het onderzoek naar de beveiliging van de Schuberg Philis infrastructuur en de IRC/LEDA applicatie, inclusief de in eind november 2019 uitgevoerde hertest. Alleen de na de hertest nog aanwezige bevindingen zijn in detail opgenomen in dit rapport.

Belangrijkste bevinding

Gedurende het onderzoek zijn tijdens de initiële testwerkzaamheden een aantal hoog, midden en laag risico kwetsbaarheden aangetroffen. […]

[…]

De details van de gedurende de hertest aangetroffen kwetsbaarheden zijn beschreven in hoofdstuk 2 van dit rapport.

2 Bevindingen en aanbevelingen

2.1 Inleiding

In dit hoofdstuk worden de bevindingen en aanbevelingen uit de pentest in detail beschreven. Wij hebben handmatig de kwetsbaarheden nagelopen die door onze testprogramma's zijn gevonden. Daarbij verifiëren wij of de kwetsbaarheden werkelijk aanwezig zijn of dat de testprogramma's valse meldingen hebben gegeven. Na de verificatie hebben wij van de aangetroffen kwetsbaarheden de risicoclassificaties bepaald en een schatting gemaakt van de inspanning die nodig is om de kwetsbaarheid te verhelpen. In bijlage 1 van dit rapport is beschreven hoe de risicoclassificaties zijn te interpreteren.

De aangetroffen kwetsbaarheden zijn in onderstaande tabel samengevat. De bij de hertest niet meer aanwezige bevindingen zijn doorgehaald. Daarnaast is een risicoclassificatie opgenomen en een indicatie over de benodigde inspanning (Insp.). Tot slot zijn de gevonden kwetsbaarheden in de laatste kolom van de tabel opgedeeld naar applicatie (A) of de infrastructuur (I), zoals de webserver of het netwerk. Hiermee wordt aangegeven op welk niveau de kwetsbaarheid zich bevindt[1].

[...]

De toelichting op de aangetroffen kwetsbaarheden is opgenomen in de volgende paragrafen. Zie voor een toelichting op alle onderzochte typen kwetsbaarheden bijlage 2.

2.2 [...]

Risico	Inspanning	Type	Soort
H	M	Component afhankelijke kwetsbaarheid	Applicatie/ Infrastructuur

[...]

Een applicatie maakt veelal gebruik van verschillende componenten. Het bekend worden van kwetsbaarheden in deze componenten kan ertoe leiden dat de

[1] Een kwetsbaarheid op applicatieniveau bevindt zich in de programmacode of configuratie van de webapplicatie. Een kwetsbaarheid op infrastructuurniveau bevindt zich op de infrastructuurlaag, bijvoorbeeld in de onderliggende webserver of aanwezige proxies.

beveiliging van de applicatie, de webserver of de database in het geding is. Tijdens de test zijn de applicatie en de onderliggende componenten onderzocht op bekende kwetsbaarheden.

Om de beveiliging van de applicatie en onderliggende componenten te verhogen is het een best practice [...]. Kwetsbaarheden kunnen de beschikbaarheid, integriteit en vertrouwelijkheid van de webapplicatie in gevaar brengen. [...].

2.3 [...]

Risico	Inspanning	Soort
L	L	Infrastructuur

[...] Deze gegevens kunnen daaropvolgend door de aanvaller gebruikt worden om te proberen in te loggen op alle in het netwerk bereikbare hosts.
[...]

3 Verantwoording onderzoek

3.1 Doelstelling en onderzoeksvragen

Doelstelling van het onderzoek is om inzicht te geven in de (mogelijke) tekortkomingen en kwetsbaarheden van de te onderzoeken Schuberg Philis Financiën-infrastructuur en de Interne Rekening-courant - Leen- en depositoadministratie (IRC/LEDA) (web)applicatie van de Rijkshoofdboekhouding (RHB), door middel van het uitvoeren van een technisch beveiligingsonderzoek inclusief hertest.

Het doel van de opdracht is bereikt als de volgende vragen zijn beantwoord:

1. *Welke kwetsbaarheden bevat de te onderzoeken infrastructuur?*
2. *Welke kwetsbaarheden bevat de te onderzoeken IRC/LEDA applicatie?*
3. *Welke beveiligingsrisico's leveren de drie te onderzoeken scenario's op (zie paragraaf 3.2)?*
4. *Welke (standaard) aanvallen (zoals bekende exploits), scans (zoals Nessus, nmap) en andere malafide acties (zoals uploaden van malware) worden gedetecteerd en welke niet?*
5. *Hoe kunnen de hiermee gepaard gaande risico's worden gemitigeerd?*

Bovenstaande vragen zijn, op vraag 4 na, beantwoord middels het uitgevoerde beveiligingsonderzoek (pentest) inclusief de eind 2019 uitgevoerde hertest […].

Vraag 4 bleek gedurende het onderzoek niet adequaat te beantwoorden, omdat we op locatie bij Schuberg Philis aan het testen waren en we dus al 'fysiek' zichtbaar waren. Hierdoor zou niet duidelijk zijn of ze daadwerkelijk onze testhandelingen zouden detecteren, of uitgaan van onze aanwezigheid en daarop signaleren dat er bepaalde handelingen op de infrastructuur worden uitgevoerd. […]

In bijlage 2 is de gedetailleerde beschrijving van de gehanteerde werkwijze opgenomen.
Tevens zijn in het rapport gerichte aanbevelingen verstrekt om de risico's bij het aantreffen van eventuele kwetsbaarheden te mitigeren.

3.2 Object van onderzoek, scope en definities

[...] Het netwerk (de infrastructuur en de daarbinnen aanwezige servers en gebruikte services, zoals Active Directory) en de IRC/LEDA applicatie zijn onderzocht op bekende kwetsbaarheden.

Uit de Business Impact Analyse is naar voren gekomen dat het verhogen van rechten binnen het netwerk als belangrijk risico is gesignaleerd. Op basis hiervan zijn in overleg met de CISO van Financiën met betrekking tot de beveiliging van het netwerk de volgende drie specifieke te onderzoeken scenario's gedefinieerd:

1. Perspectief van een 'malicious' insider, d.w.z. wat kan een kwaadwillende Financiën of SBP-medewerker binnen het netwerk;
2. Perspectief van een 'malicious' outsider, d.w.z. wat kan een kwaadwillende buitenstaander binnen het netwerk;
3. Het uploaden dan wel verspreiden van malware door een 'malicious insider'.

Verder heeft het beveiligingsonderzoek op IRC/LEDA zich gericht op de mogelijkheden tot het ongeautoriseerd inzien en wijzigen van gegevens (de kwaliteitsaspecten vertrouwelijkheid en integriteit).

Tot slot is gevraagd om te proberen (een deel van) de security testen onopvallend uit te voeren [...].

Verandering in de scope

Zoals in 3.1 aangegeven, bleek het onopvallend testen en zo detectietechnieken te testen gedurende het onderzoek minder relevant, omdat we op locatie bij Schuberg Philis aan het testen waren en dus al 'fysiek' zichtbaar waren.

3.3 Aanpak en werkwijze

Het onderzoek van de infrastructuur en de applicatie is opgebouwd uit meerdere fasen, namelijk verkenning, testen en analyse. Een uitgebreide beschrijving van de gehanteerde aanpak is opgenomen in bijlage 2 van dit rapport.

Dit onderzoek is uitgevoerd verspreid over 2019, grotendeels op locatie bij SBP. De initiële testen zijn uitgevoerd in Q1, daarna is in Q3 aanvullend onderzoek verricht en de hertest is in Q4 uitgevoerd.
De initiële bevindingen uit dit onderzoek zijn in Q1 en Q2 2019 afgestemd met de betrokkenen. De resultaten van de hertest zijn op 3 december 2019 per mail afgestemd met de betrokkenen van MinFin (namens de opdrachtgever) en SBP.

3.4 Gehanteerde Standaard

Deze onderzoeksopdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing (IIA standaarden).

Voor alle duidelijkheid geven wij aan dat wij geen assurance-opdracht uitvoeren en derhalve geen zekerheid geven over het object van onderzoek. Er is volstaan met het rapporteren van de onderzoeksresultaten. Het is aan de opdrachtgever zelf om op basis van de uitkomsten van ons onderzoek een oordeel te vormen.

3.5 Verantwoording uitkomsten

De uitkomsten van dit beveiligingsonderzoek zijn indicatief en geven geen oordeel (assurance) over het beveiligingsniveau en beheer van de onderzochte infrastructuur en applicatie. Kwetsbaarheden kunnen vaak, door de beperkte tijd en middelen, niet zover worden onderzocht dat het mogelijk wordt ze volledig uit te buiten. Gedurende de onderzoeksperiode is met diverse hulpmiddelen getest op de belangrijkste kwetsbaarheden. Een aanvaller met onbeperkte tijd en middelen zal een grotere kans hebben om de beveiliging uiteindelijk te doorbreken. Daarnaast spelen de continu voortschrijdende technologische ontwikkelingen en wijzigingen op de infrastructuur en applicatie een rol. Daarom blijft een constante alertheid ten aanzien van de beveiliging noodzakelijk.

3.6 Verspreiding rapport

De opdrachtgevers Hoofd Eenheid Informatisering en Afdelingshoofd RHB, zijn eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgevers met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt.

In afstemming met de opdrachtgever wordt het ADR-rapport gerubriceerd als departementaal vertrouwelijk. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website. Het ADR-rapport zal ook op deze lijst worden vermeld. Het ADR-rapport zal niet op de website van de rijksoverheid worden geplaatst conform standaard beleid gezien de departementaal vertrouwelijke status.

4 Ondertekening

Den Haag, 25 november 2020

[...]

Projectleider
Auditdienst Rijk

Bijlage 1 – Toelichting risicobeschrijving

In dit rapport zijn risicoclassificaties opgenomen om de bevindingen te categoriseren. In Tabel 1 hebben wij de gehanteerde risicoclassificatie opgenomen. Daarnaast geven wij per bevinding een schatting aan van de benodigde inspanning om de bevinding te verhelpen. In Tabel 2 hebben wij de gehanteerde inspanningsclassificatie opgenomen.

Classificatie	Risico
Hoog (**H**)	Een bevinding met hoog risico betreft een situatie die direct kan leiden tot het schaden van de integriteit, vertrouwelijkheid en/of beschikbaarheid van gegevens en/of systemen. Hoge risico's dienen zo snel mogelijk gemitigeerd, of beter nog, te worden verwijderd.
Midden (**M**)	Een bevinding met midden risico betreft een situatie die niet op zichzelf de mogelijkheid biedt tot het schaden van de integriteit, vertrouwelijkheid en/of beschikbaarheid van gegevens en/of systemen. Wel biedt het een mogelijkheid, of verschaft het de informatie, om dat in combinatie met andere hulpmiddelen of informatie *eenvoudig* te bereiken. Middelmatige risico's verdienen ook de aanbeveling om te mitigeren of te verwijderen, maar hebben geen directe urgentie.
Laag (**L**)	Een bevinding met laag risico betreft een situatie die niet op zichzelf de mogelijkheid biedt tot het schaden van de integriteit, vertrouwelijkheid en/of beschikbaarheid van gegevens en/of systemen. Wel biedt het een mogelijkheid, of verschaft het informatie, om dat in combinatie met andere hulpmiddelen of informatie te bereiken. Lage risico's dienen overwogen te worden om te mitigeren of te verwijderen.

Tabel 1: Classificatie van risico's

Classificatie	Inspanning
Hoog (**H**)	Een aanbeveling die hoge inspanning vereist, omvat omvangrijke onderzoek- en implementatieactiviteiten.
Midden (**M**)	Een aanbeveling die middelmatige inspanning vereist, omvat middelmatige onderzoeks- en implementatieactiviteiten.
Laag (**L**)	Een aanbeveling die lage inspanning vereist, omvat geringe onderzoeks- en implementatieactiviteiten.

Tabel 2: Classificatie van benodigde inspanning

Bijlage 2 – Gedetailleerde fasering onderzoek

De aanpak is opgesplitst in twee delen: onderzoek naar het SBP Financiën-netwerk inclusief koppelingen met IT-specials enerzijds en onderzoek naar de IRC/LEDA-webapplicatie (schatkistbankieren) anderzijds. Het onderzoek is uitgevoerd vanuit het Ministerie van Financiën, locatie Korte Voorhout 7 voor de testen vanaf het Internet. Voor de infrastructuur gerelateerde testen, testscenario's met betrekking tot de mogelijkheden op het netwerk, en de test op de acceptatieomgeving van IRC/LEDA is getest op locatie bij SBP.

Onderzoek SBP Financiën-netwerk inclusief koppeling met IT-specials
Wij hebben door middel van geautomatiseerde en handmatige testen onderzocht of het mogelijk is om binnen te dringen in de systemen binnen het SBP-netwerk, welke (vertrouwelijke) informatie toegankelijk is, welke handelingen kunnen worden uitgevoerd, of het mogelijk is 'verhoogde rechten' (beheerrechten) te verkrijgen en of malware in de omgeving kan worden geplaatst en eventueel verspreid.

De belangrijkste onderwerpen die tijdens de testen op het netwerk aan de orde komen, zijn:

- Toegankelijke services. De in het netwerk aangeboden services zouden aanvallers de mogelijkheid kunnen geven om ze te misbruiken teneinde toegang te krijgen tot servers. Dit kan bijvoorbeeld door het lekken van bepaalde gevoelige informatie en/of zwakheden in de configuratie. Tijdens de test wordt gezocht naar services die mogelijk misbruikt kunnen worden.
- Bestands- en directory toegang. De op de servers aanwezige bestanden bieden aanvallers mogelijk extra informatie om de servers aan te vallen. Dit geldt zowel voor bestanden die alleen informatie bevatten als voor programma's, scripts en tools voor test- of beheerdoeleinden. Tijdens de test wordt gezocht naar veel voorkomende bestanden en directories.
- Component afhankelijke kwetsbaarheden. Binnen een netwerk wordt veelal gebruik gemaakt van verschillende componenten. Het bekend worden van kwetsbaarheden in deze componenten kan ertoe leiden dat de beveiliging van (onderdelen van) het netwerk in het geding is. Tijdens de test worden bekende kwetsbaarheden getest op de in het netwerk aanwezige componenten.

- Authenticatiemechanismen. Binnen een netwerk wordt gebruik gemaakt van een of meer authenticatiemechanismen om toegang te krijgen tot bepaalde delen van het netwerk en/of componenten (zoals servers) daarin. De sterkte van de gebruikte mechanismen bepaalt voor een groot deel het beveiligingsniveau van het netwerk. Tijdens de test wordt onderzocht of adequate authenticatiemechanismen worden toegepast, of mogelijkheden aanwezig zijn om de beveiliging te omzeilen of om kwetsbaarheden van een gebruikt authenticatiemechanisme aan te tonen, onder door het toepassen van relaying en pass-the-hash technieken.
- Netwerksegmentatie. Netwerken worden vaak gescheiden in netwerksegmenten voor ondermeer beveiligingsdoeleinden en performance. Tijdens de test wordt nagegaan welke netwerkcomponenten de netwerkscheiding tot stand brengen en of het mogelijk is om controles aangebracht in of via deze netwerkcomponenten te omzeilen om zodoende toegang te verkrijgen tot (systemen in) andere netwerksegmenten.

Het onderzoek naar de beveiliging van het SBP Financiën-netwerk is globaal opgebouwd uit de volgende vier fasen:

Fase 1 - bestaat uit een verkenning van het netwerk inclusief de koppelingen en de daarbinnen gebruikte componenten en technieken. Het netwerk wordt door onder andere afluisteren van netwerkverkeer en portscanning in kaart gebracht. Ook wordt hierbij gesteund op de door SBP aangeleverde Laag 3, Laag 7 en architectuur documenten van de infrastructuur.

Fase 2 - bestaat uit het (geautomatiseerd) testen van het netwerk. Het netwerk zal handmatig en met behulp van onze testprogramma's worden getest op bekende kwetsbaarheden die mogelijk in het netwerk aanwezig zijn, op bijvoorbeeld servers en netwerkcomponenten.

Fase 3 – bestaat uit het onderzoeken naar kwetsbaarheden in de beveiliging vanuit de drie te onderzoeken scenario's, zoals deze zijn benoemd in de scope van het onderzoek in bijlage 1.

Er zijn hierbij geen daadwerkelijk kwaadaardige bestanden ingezet die systemen en/of data beschadigen.

Fase 4 - is een analyse van de resultaten die onze tests hebben opgeleverd en mogelijke daarop gebaseerde vervolgacties. Het is mogelijk dat tests zogenaamde "false positives" opleveren waarbij het lijkt dat een risico aanwezig is, terwijl dit in feite niet het geval is. Om "false positives" zoveel mogelijk uit te sluiten worden alle resultaten handmatig onderzocht.

Onderzoek webapplicatie IRC/LEDA

Wij hebben door middel van geautomatiseerde en handmatige testen onderzoeken of het mogelijk is de functionaliteit van de IRC/LEDA webapplicatie te misbruiken of binnen te dringen in de applicatie of de onderliggende systemen, zoals de databases. De aanwezigheid van de beveiligingsmaatregelen zijn zowel handmatig als met behulp van gespecialiseerde software getest.

De belangrijkste onderwerpen die tijdens de (geautomatiseerde) testen aan de orde komen zijn:

- Bestands- en directory toegang. De op de servers aanwezige bestanden bieden aanvallers mogelijk extra informatie om de servers aan te vallen. Dit geldt zowel voor bestanden die alleen informatie bevatten als voor programma's voor test- of beheerdoeleinden. Tijdens de test wordt gezocht naar veel voorkomende bestanden en directories.
- Controle van invoervariabelen. Aandacht voor de controle van invoervariabelen is bij webapplicaties van groot belang. De programmeur moet ervan uitgaan dat alle invoer onbetrouwbaar is. De bezoeker van de website valt buiten de invloedssfeer van de organisatie en kan daarmee niet gebruikt worden om invoer te controleren, dit moet op de server gebeuren. Tijdens de test wordt foutieve invoer aangeboden om te zien hoe de webapplicatie hiermee omgaat.
- Component afhankelijke kwetsbaarheden. Een webapplicatie maakt veelal gebruik van verschillende componenten. Het bekend worden van kwetsbaarheden in deze componenten kan ertoe leiden dat de beveiliging van de applicatie, de webserver of de database in het geding is. Tijdens de test worden bekende kwetsbaarheden getest op de applicatie en de onderliggende componenten.
- Beveiligingsmechanisme. Een webapplicatie kan gebruik maken van een beveiligingsmechanisme als vertrouwelijke en/of persoonlijke gegevens kunnen worden ingevoerd of geraadpleegd. De sterkte van dit mechanisme bepaalt voor een groot gedeelte het beveiligingsniveau van de webapplicatie. Tijdens de test wordt onderzocht of een adequaat beveiligingsmechanisme is toegepast, of mogelijkheden aanwezig zijn om de beveiliging te omzeilen of om kwetsbaarheden van een gebruikt beveiligingsmechanisme aan te tonen.
- Beveiliging gegevenstransport. De verbinding met de webapplicatie wordt vaak afgeschermd door middel van SSL-certificaten zodat vertrouwelijke gegevens niet door derden kunnen worden onderschept. Het type en de configuratie van de gebruikte certificaten bepalen voor een belangrijk gedeelte het beveiligingsniveau van de communicatie tussen gebruiker

en webapplicatie. Gedurende de test wordt nagegaan of op de noodzakelijke plekken gebruik wordt gemaakt van certificaten en of deze veilig zijn geïmplementeerd.

- Security headers. HTTP response headers kunnen worden gebruikt om een stuk client-side beveiliging te regelen via de browser van de gebruiker. Ze kunnen bijvoorbeeld aangegeven hoe de applicatie benaderd dient te worden, waar de inhoud vandaan mag komen en wat voor soort inhoud getoond mag worden. Het instellen van dergelijke security headers vindt plaats via de webserver, die ze in elke response richting de gebruiker meegeeft.

Het beveiligingsonderzoek naar de IRC/LEDA webapplicatie is opgebouwd uit de volgende drie fasen:
Fase 1 - bestaat uit een verkenning van de webapplicatie en infrastructuur, en de daarbinnen gebruikte technieken. De functionaliteit van de applicatie wordt met een reguliere browser verkend. [...]
Fase 2 - bestaat uit het (geautomatiseerd) testen van de applicatie. De webapplicatie zal handmatig en met behulp van onze testprogramma's worden getest op kwetsbaarheden van de webserver, het applicatieplatform en de programmacode.
Fase 3 - is een analyse van de resultaten die onze tests hebben opgeleverd en mogelijke daarop gebaseerde vervolgacties. Het is mogelijk dat tests zogenaamde "false positives" opleveren waarbij het lijkt dat een risico aanwezig is, terwijl dit in feite niet het geval is. Om "false positives" zoveel mogelijk uit te sluiten worden alle resultaten handmatig onderzocht.

Wij hebben geen Denial of Service (DoS) aanval gesimuleerd door grote hoeveelheden verkeer te genereren, wel hebben we getest op kwetsbaarheden die mogelijk een DoS kunnen veroorzaken.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00