Rekenkamerbrief Digitale Veiligheid

1. Inleiding

In het voorjaar en de zomer van 2019 hebben de Rekenkamer Leudal en de CISO (Chief Information Security Officer) van de gemeente Leudal ethische hackers verzocht een onderzoek te doen naar de digitale veiligheid van de gemeente Leudal. De onderzoeken zijn onafhankelijk van elkaar opgestart, doch met kennis van elkaars bestaan, en later met elkaar besproken. Deze onafhankelijkheid zorgt er voor dat verschillende invalshoeken met betrekking tot digitale veiligheid aanvullend naast elkaar hun werk hebben kunnen doen en elkaar daardoor ook hebben kunnen versterken. Bovendien kijken een CISO en een Rekenkamer vanuit hun doelstellingen verschillend naar een zelfde praktijk, wat in de uitwerking een versterkende en synergetische uitwerking kan hebben.

Bespreking van elkaars onderzoeken heeft er toe geleid dat de Rekenkamer Leudal een rapportage, deze rekenkamerbrief, heeft opgesteld ten behoeve van de informatievoorziening aan de gemeenteraad van de gemeente Leudal, waarbij doelstellingen, werkwijzen, bevindingen, conclusies en aanbevelingen van beide onderzoeken geïntegreerd zijn opgenomen. Deze rapportage is dan ook geheel en al de verantwoordelijkheid van de Rekenkamer Leudal.

Bevindingen met een daadwerkelijk veiligheidsrisico zijn in deze rapportage in algemene bewoordingen opgeschreven zonder dat voor buitenstaanders direct herleidbaar is waar bepaalde risico's zich zouden kunnen bevinden. Deze risico's zijn de CISO van de gemeente Leudal bekend en zijn tussen de onderzoekperiode en verslagperiode direct opgepakt.

Omdat digitale veiligheid een terugkomend aandachtspunt is, ook vanuit de aankomende Baseline Informatieveiligheid Overheid (onderdeel van de Digitale Agenda 2020), en dit een ieder frequent aan gaat binnen de gemeente Leudal, hebben de bevindingen en daar aan verbonden conclusies en aanbevelingen van deze rekenkamerbrief ook hun kracht naar de toekomst toe. Zowel ten aanzien van de technologische zijde van de digitale infrastructuur van de gemeente Leudal, als naar het gedrag van de gebruikers van deze digitale infrastructuur. En met dit laatste bedoelen we natuurlijk "ik en u"! En niemand uitgezonderd!

In het vervolg van deze rekenkamerbrief gaan we nader in op het doel van de onderzoeken, de terreinen van onderzoek, de toegepaste werkwijze en de verschillende bevindingen. We eindigen de rekenkamerbrief met de conclusies en aanbevelingen.

2. Doel van de onderzoeken

Het doel van de onderzoeken was een graadmeting te verkrijgen binnen de gemeente Leudal en al haar stakeholders van de algehele gesteldheid op het gebied van de digitale veiligheid. Om hiermee ook inzicht te krijgen in de risico's en kwetsbaarheden van de onderzochte systemen en websites, de beveiliging te verbeteren, en zodoende ook de kwetsbaarheden te kunnen bestrijden. De nadruk ligt daarbij op de bescherming van persoonsgegevens en ongeautoriseerde toegang tot de systemen van de gemeente Leudal.

Met de uitgebreide technische rapportages zijn de verantwoordelijken in staat actie te ondernemen om de veiligheid van de digitale infrastructuur te verbeteren, alsmede het gedrag van de gebruikers van de digitale infrastructuur van de gemeente Leudal op een zodanige wijze te beïnvloeden, dat uit

hun handelingen geen onnodige risico's voor de digitale veiligheid van de gemeente Leudal voortvloeien.

Tevens was het doel om vast te stellen of de gevonden problemen incidenteel of structureel zijn.

- Incidentele problemen ontstaan veelal als er af en toe buiten de gebaande paden vernieuwingen of aanpassingen worden gedaan aan de ICT-infrastructuur. Dit gebeurt veelal onder (tijds)druk en door het niet volgen van protocollen en processen en dit leidt dan mogelijk tot zwakte in veiligheid.
- Structurele problemen ontstaan veelal door het ontbreken van protocollen, processen en triggers. Een softwaresysteem of applicatie dient bijvoorbeeld regulier bijgewerkt te worden. Dat dient te gebeuren vanuit processen. Als dat echter gebeurt vanuit een onverwachte trigger doordat er technisch of functioneel iets "niet meer goed werkt" dan is er een structureel probleem. De oorzaken van structurele problemen zijn vaak tijdgebrek, geldgebrek, capaciteitsgebrek of prioriteitsgebrek.

3. Onderdelen van het onderzoek

De Security Scans voor Gemeente Leudal, zoals uitgevoerd door de CISO van de gemeente Leudal en de Rekenkamer Leudal bestonden uit de volgende onderdelen:

- Remote scan
- Phishing campagne
- Lokale digitale penetratietest
- E-mail header spoofing test
- Wifi scan
- USB pentest.

In de onderzoeken zijn alle bij de gemeente Leudal behorende domeinen (*.leudal.nl) en haar sub domeinen meegenomen. Dat betekent dat alle technische onderdelen die betrokken zijn meegenomen werden, zoals: servers, pc's, systeemsoftware en applicaties.

Daarnaast heeft een e-mail campagne plaatsgevonden, waarbij het leek of verschillende personen uitnodigingen hadden verstuurd aan medewerkers van onze organisatie. En is een 'e-mail header spoofing test' opgenomen. Hierin wordt onderzocht of de e-mailservers van de gemeente Leudal juist handelen, indien een externe kwaadwillende zich in het e-mailverkeer van de gemeente voor doet als een gebruiker met een '@leudal.nl' e-mailadres.

Als laatste is op locatie de beveiliging getest, het netwerk onderzocht en hebben er op diverse plekken USB sticks gelegen. Tijdens deze testen is op bovengenoemde punten onderzocht welke inbreuk er gemaakt kon worden aan -, op - of bij de digitale infrastructuur van de gemeente Leudal. Tijdens deze testen wordt op bovengenoemde vlakken onderzoek gedaan naar de mogelijkheid schade aan te richten aan, of binnen te dringen bij de digitale infrastructuur van de gemeente Leudal.

4. Onderzoeksmethode

Vooraf is in beide onderzoeken bepaald dat de nodige zorgvuldigheid in acht werd genomen om geen schade of ongewenste uitval te veroorzaken. In beide onderzoeken is vervolgens volgens de 'Blackbox' methode gewerkt. Dat wil zeggen dat zowel de CISO als de Rekenkamer Leudal geen gegevens hebben verstrekt aan de opdrachtnemer, om op deze manier zo dicht mogelijk bij de werkelijkheid van een echte hacker te komen. Ook zijn de beide ethische hackers niet geïnformeerd over elkaars activiteiten.

De aanpak van de onderzoeken bestonden uit een aantal stappen, die door beide ethische hackers voor een deel zijn opgepakt, doch bij elkaar opgeteld integraal hebben plaatsgevonden.

- **Informatiefase;** Tijdens deze fase (ook wel Reconnaissance genoemd) wordt gepoogd zo veel mogelijk technische en persoonlijke informatie te achterhalen uit openbare bronnen zoals sociale media (e-mailadressen, namen medewerkers, functies, gebruikte systemen, beheerpartijen, e.d.) en de domeinen binnen de reikwijdte van de penetratietest van de (ethische) hackers door contact te maken met de bijbehorende systemen.
- **Analysefase;** De gevonden informatie wordt gebruikt om een index op te stellen van mogelijke kwetsbaarheden, hiermee zal de aanvalsstrategie worden bepaald.
- **Aanvalsfase;** De kwetsbaarheden worden getest.
    - **Stap 1: Delivery**.
      De aanvaller stuurt de kwaadaardige link of bestand naar het slachtoffer. Dit gebeurt in de meeste gevallen via de mail[1].
    - **Stap 2: Exploitation**.
      De uiteindelijke uitvoering van de exploit door de aanvaller.
    - **Stap 3: Installation**.
      De aanvaller zorgt ervoor dat de kwaadaardige code ook uitgevoerd wordt als het slachtoffer heeft afgemeld en de dag erna weer aanmeldt.
    - **Stap 4: Command and Control**.
      Als het slachtoffer op de kwaadaardige link klikt of het kwaadaardige bestand opent, wordt de kwaadaardige code uitgevoerd en neemt de aanvaller het systeem over.
    - **Stap 5: Lateral Movement**.
      Is het doelsysteem eenmaal overgenomen, dan kan de aanvaller zijn aandacht richten op andere systemen in het netwerk. Zijn hier nog meer systemen te vinden die kunnen worden overgenomen?
    - **Stap 6: Actions on objectives**.
      De aanvaller voert acties uit om de doelstelling te realiseren.
- **Verder onderzoek;** Indien een kwetsbaarheid tot verdere toegang heeft geleid wordt de hier verkregen nieuwe informatie opnieuw geanalyseerd en onderzocht op mogelijke veiligheidsproblemen.

[1] Waar beveiligingsrisico's heel vaak optreden en waar het gedrag van de medewerker cruciaal is met betrekking tot het openbaren van deze risico's is vooral gelegen in het gebruik van e-mail.

5. Bevindingen

Uit de onderzoeksmethoden van beide ethische hackers komen een aantal bevindingen naar voren. We zullen deze bevindingen ordenen naar ICT-infrastructuur en E-mail, dat wil zeggen naar het onderscheid tussen technische digitale veiligheid en antropologische digitale veiligheid. Met dat laatste bedoelen we feitelijk het gedrag en de beïnvloeding van het gedrag van de betrokken gebruikers van de digitale infrastructuur in de gemeente Leudal.

5.1. Technische digitale veiligheid

Remote test

De digitale of ICT-infrastructuur is het geheel van hardware, software, applicaties en netwerken in de gemeentelijke organisatie. De technische inrichting van de website www.leudal.nl is over het algemeen goed op orde. Er zijn echter wel een aantal systemen met potentiële veiligheidsrisico's aangetroffen, waardoor de mogelijkheid bestaat om op een ongeoorloofde wijze toegang te krijgen tot de websites. Veel inzet van een kwaadwillende zou hierbij kunnen leiden tot een digitale inbraak.

Daarnaast zijn er op sommige systemen verschillende problemen aangetroffen met de beveiligde verbinding. Dit varieert van grote problemen, zoals het ontbreken van een geldig veiligheids-certificaat tot kleinere problemen, zoals het toelaten van verouderde versleutelingsmethodes. Een kwaadwillende kan de problemen met de beveiligde verbindingen mogelijk uitbuiten om de gegevens tussen de website en zijn bezoekers af te luisteren of aan te passen.

Op de website www.leudal.nl zijn openbare documenten uit 2018 aangetroffen die in sommige gevallen gemaakt zijn met verouderde versies van Microsoft Office pakketten, wat kan wijzen op het gebruik van deze verouderde software op systemen binnen het interne netwerk van de gemeente Leudal. Bij het contactformulier op de website kunnen bestanden meegestuurd worden, hier worden de verouderde bestandsformaten '.doc' en '.ppt' toegestaan. Dit kan eveneens duiden op het gebruik van verouderde software op de computers van medewerkers die deze formulieren afhandelen. Wanneer dit zo is dan kan een kwaadwillende van het contactformulier misbruik maken om een bestand met schadelijke code bij een medewerker van de gemeente aan te bieden. Wanneer dit document wordt geopend kan de kwaadwillende de computer overnemen.

Lokale penetratietest

De ethische hackers hebben moeite gehad met toegang behouden op het netwerk, vanwege de inrichting van de infrastructuur van de gemeente Leudal. Het vasthouden van de verbinding wordt verbroken, wanneer een gebruiker uitlogt. De volgende dag staat een schone desktop klaar zonder malware. Het netwerk van Gemeente Leudal is gesegmenteerd, dit houdt in dat het netwerk opgedeeld is in kleinere netwerken, wat de performance en beveiliging ten goede komt. Wederom een bevestiging dat de technische infrastructuur van de gemeente Leudal over het algemeen op orde is.

Echter wanneer men toegang heeft tot het netwerk (en de technische kennis), dan zijn er toch verschillende acties uit te voeren, die feitelijk niet zouden mogen gebeuren. Hiermee is de CISO dan ook direct aan de slag gegaan.

Omdat er oude documenten op locaties zijn gevonden, met wachtwoorden erin, kon er servertoegang worden verkregen. Er zijn enkele taken gestart op enkele servers, die elke x-periode verbinding met de infrastructuur van de ethische hackers maakten. Deze zijn meerdere malen gedetecteerd door medewerkers, maar er is niet adequaat op gereageerd, waardoor de inbreuk kon blijven voortduren.

Daarnaast is door middel van ontsleuteling-software ingebroken in bestanden met gebruikersnamen en wachtwoorden, waarbij van een groot aantal gebruikersnamen en wachtwoorden er binnen 3 dagen 78% zijn ontsleuteld. Er werden merendeels dezelfde wachtwoorden gevonden.

Wifi scan
Er zijn in Leudal 3 netwerken beschikbaar; Leudal, Leudal-Gast en Raadsleden. Er is op verschillende manieren getracht inbreuk te maken op de netwerken. Het Leudal netwerk is afdoende beveiligd voor inbreuk van buitenaf. Het Leudal-Gast netwerk is een onbeveiligd openbaar netwerk. Opmerking hierbij is, dat dit netwerk door zowel bezoekers, als ook apparatuur van medewerkers gebruikt kan worden. Vanwege de hoge intensiteit van draadloze apparatuur, is het praktisch onmogelijk om in Leudal inbreuk te maken via dit netwerk. Van belang is te beseffen dat wanneer gebruik wordt gemaakt van openbare netwerken op andere locaties, dit altijd een risico met zich meebrengt, wanneer op andere locaties hackers actief zijn. Er bestaat apparatuur, die op elke aanvraag een connectie laat maken, ook als dit malafide is. Het Raadsleden netwerk maakt gebruik van een ouder beveiligd netwerkprotocol, waarbij het wachtwoord meegegeven wordt. In dit netwerk kunnen alle servers benaderd worden. Ook dit veiligheidsrisico is in de tussentijd opgepakt.

5.2. Antropologische digitale veiligheid

Phishing campagne
Bij een aanval op een digitale infrastructuur wordt eerst informatie verzameld omtrent de gebruikers van de Gemeente Leudal. Met behulp van Phishing wordt de gebruiker nieuwsgierig gemaakt om door middel van een link in een mail de gewenste malware op te starten of zijn/haar aanmeldgegevens prijs te geven. Phishing is een techniek waarbij iemand een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken. De aanval is erop gericht om vertrouwelijke of geheime informatie los te krijgen, waarmee de hacker dichter bij het aan te vallen object kan komen. Kenmerkend voor Phishing is dat er geen aanval op de techniek zelf wordt uitgevoerd. Een aanvaller tracht de nieuwsgierigheid van een slachtoffer te wekken, medelijden bij een slachtoffer te wekken of een slachtoffer bang te maken.

In de onderzoeken is een dergelijke phishing-techniek ingezet. Hierbij heeft ongeveer 10% van de personen aan wie een vervalste mail was gestuurd hun gebruikersnaam en wachtwoord ingegeven op een malafide website, waardoor ze de mogelijkheid hebben geboden om de digitale infrastructuur van de gemeente Leudal binnen te laten dringen. Hierna is een zogenoemde ‘Spear-Fishing’ toegepast op 10% gebruikers, waarbij de ethische hacker gebruik heeft gemaakt van op internet aanwezige informatie over deze personen. Zo heeft hij ze verleid om te klikken op kwaadaardige links, waarbij toegang tot het netwerk van de gemeente Leudal is verkregen.

E-mail header spoofing
Tijdens het onderzoek bleek het ook mogelijk om succesvol een 'header spoofing' aanval uit te voeren. Dit houdt in dat een externe kwaadwillende zich in het e-mailverkeer van de gemeente kan voordoen als een gebruiker met een @leudal.nl e-mailadres. Zo is het voor een externe persoon op dit moment mogelijk om, zonder toegang te hebben of hiertoe geautoriseerd te zijn, een e-mail te versturen van elk mogelijk @leudal.nl e-mailadres aan een ontvanger met een @leudal.nl e-mailadres. De externe persoon kan er bijvoorbeeld voor kiezen een e-mail te sturen met als afzender info@leudal.nl aan elke @leudal.nl gebruiker. Dit zouden ook e-mailadressen van bestaande gebruikers kunnen zijn, zoals het e-mailadres van de burgemeester, waardoor ontvangers van deze email daadwerkelijk zouden kunnen denken de inhoud van de email ook uit te voeren. Dit kan ernstige consequenties hebben, zoals vergelijkbare onderzoeken in andere gemeenten hebben aangetoond. Ook dit vraagstuk is door de CISO direct opgepakt.

USB penetratietest
Voor de USB penetratietest zijn er 3 USB sticks in de organisatie gebracht. Wanneer deze sticks zouden worden ingestoken, dan zou er schadelijke software worden gestart, waardoor de werkplek overgenomen kan worden. 1 memorystick is gevonden en aangemeld als beveiligingsincident, niet ingestoken. Deze is daarna nogmaals de organisatie ingebracht en daarna wederom aangemeld als beveiligingsincident en niet ingestoken. 1 memorystick is alleen verplaatst, niet ingestoken. De laatste memorystick is aangemeld als beveiligingsincident. Bij onderzoek van het incident wordt aangegeven door de melder, dat de stick niet is ingestoken, terwijl later in overleg met de ethische hacker wel blijkt dat de stick is ingestoken.

Andere bevindingen

Naast de bovenstaande bevindingen is met betrekking tot het gebruik van e-mail geconstateerd, dat het voorkomt dat medewerkers die nog niet in dienst zijn toch een email-adres (account) van de gemeente Leudal krijgen. Gegeven de bovenstaande risico's van phishing en spoofing is het aan te raden dit niet te doen.

6. Conclusies en aanbevelingen

6.1. Conclusies

De gemeente Leudal heeft technisch gezien de zaken goed voor elkaar wat betreft hun website *www.leudal.nl*, deze is up-to-date en goed afgeschermd. Veel van de overige gevonden systemen behoeven wél aandacht vanwege een aantal verouderde software-onderdelen en een aantal problemen met de beveiligde verbindingen op deze systemen. Deze systemen dienen te worden bijgewerkt, wat inmiddels ook gebeurd is.

Daarnaast is de configuratie van de e-mailserver verbeterd, zodat het niet meer is toegestaan voor onbevoegden om zich voor te doen als een medewerkers binnen het e-mailverkeer van de gemeente.

Aan de hand van de resultaten van de uitgevoerde testen, mag worden geconcludeerd dat het Gemeente Leudal netwerk zonder blijvende aandacht niet voldoende beveiligd is. Het risico dat een kwaadwillend iemand binnen kan dringen is groot, als niet blijvend onderhoud op digitale veiligheid

wordt uitgevoerd en er periodiek sprake is van penetratietesten door wisselende ethische hackers, zodat verschillende aspecten van digitale veiligheid en hacktechnieken blijvend aandacht krijgen.

Positief is dat houvast krijgen in het netwerk moeilijk is. Wanneer echter houvast is gekregen in het netwerk, dan is er te weinig aandacht voor monitoring en controle op dagelijkse gegevensstromen, waardoor diefstal - of misbruik van gegevens of inbreuk op de privacy te laat – of niet gedetecteerd worden.

Toegang tot gevoelige informatie met betrekking tot de installatie van software is voor “normale” gebruikers mogelijk, in het bijzonder door phishing-technieken waardoor grote verstoringen kunnen optreden in de bedrijfsvoering.

Naast technische digitale veiligheid voor de digitale infrastructuur bestaan er binnen de gemeente Leudal aanzienlijke risico’s door onvoorzichtig gebruik van de digitale infrastructuur door de gebruikers. In het bijzonder in het gebruik van en toegang tot email. Gebruikersrisico’s die aanzienlijk zijn en in het bijzonder gevoelig voor phishing. Daarbij dient in ogenschouw te worden genomen dat deze risico’s groter zijn, naarmate de tijd van de medewerkers schaarser is voor dit soort zaken. In het bijzonder gaat het daarbij om gebruikers die betrokken zijn bij de verschillende besluitvormingsprocessen in de organisatie.

6.2. Aanbevelingen

Bij de aanbevelingen moet altijd rekening gehouden worden met risico, doel en middelen. Daarnaast moet er een balans worden gevonden tussen gebruiksgemak, werkbaarheid en veiligheid. Wanneer een maatregel wordt genomen op een hoog risico proces met een hoge mate van veiligheid, dan zijn ook vaak de kosten voor de te nemen maatregelen hoog.

Op basis van de bevindingen en conclusies uit de onderzoeken naar de digitale veiligheid door de CISO en de Rekenkamer Leudal komen we als Rekenkamer tot de volgende aanbevelingen:

1. De Baseline Informatieveiligheid Overheid met haar nadruk op periodiek onderhoud, inclusief testen van de digitale infrastructuur door ethische hackers, dient zonder omzien gevolgd te worden, waardoor:
    a. Systemen met sterk verouderde software worden uitgeschakeld of bijgewerkt naar huidige versie.
    b. Verouderde software op gevonden systemen vernieuwd kan worden.
    c. Problemen met de veiligheidscertificaten op de gevonden systemen worden opgelost.
    d. ‘E-mail Header Spoofing’ niet wordt toegestaan.
    e. Sprake is van een doorlopende controle op webservices;
    f. De kwaliteit van firewalls, virusscanners en netwerkconfiguraties doorlopend gemonitord wordt
2. Gebruik 2 factor authenticatie; Dit is een extra stap om in te kunnen loggen in een omgeving (in Leudal in gebruik), maar ook in apps en via websites, die buiten het Leudal netwerk

worden gebruikt of aangeboden. Het bestaat uit een wachtwoord of een pincode en een extra token, welke elke 30 seconden opnieuw gegenereerd wordt.

3. Controleer continue servers, delen van servers en werkstations op bestanden met bepaalde bestandformaten.

4. Sla fraudegevoelige documenten niet langer dan noodzakelijk op op het netwerk. Beter nog om deze op te slaan in 'beveiligde' applicaties.

5. Verhoog diverse vormen van bewustwording van digitale veiligheidsrisico's met betrekking tot phishing mail en overige digitale gevaren, zoals te simpele wachtwoorden; Gebruikers dienen permanent herinnerd te worden aan de gevaren en het achteloos klikken op links in e-mails, bijvoorbeeld met een periodiek verplichte workshop of korte boodschappen bij het opstarten van een computer.

6. Gebruik sterke wachtwoorden; Maak wachtwoorden van minimaal 20 karakters; gebruik daarvoor een wachtwoordmanager met 2 factor authenticatie en gebruik voor elke dienst of inlog een ander wachtwoord. Stuur ook geen wachtwoorden via mail, maar gebruik twee verschillende communicatiekanalen.

7. Maak geen email-accounts aan voor niet-medewerkers, ook niet als zij binnen afzienbare tijd in dienst komen.

8. Autoriseer en bekrachtig periodiek de bevoegdheden van de CISO met betrekking tot de veiligheid van de digitale infrastructuur van de gemeente Leudal. Deze bevoegdheid kent met betrekking tot vraagstukken van digitale veiligheid in de gemeente Leudal een absoluut karakter.