Security Scan

Gemeente Vaals

11/10/2007

In opdracht van de rekenkamercommissie van de gemeente Vaals is er bij de gemeente in Vaals een security scan uitgevoerd. Tijdens dit bezoek is gekeken naar zowel de fysieke als logische beveiliging van het netwerk.

Opdrachtgever:
Rekenkamercommissie Vaals
t.a.v.
Dhr. Bindels
Maastrichterlaan 136
6291 EV Vaals
Tel.: +31 43 3065490

Opdrachtnemer:
NID Solutions
Nieuw Eyckholt 300
6419 DJ Heerlen
Tel.: +31 (0) 45-4006060

Contents

1. Samenvatting

In opdracht van de rekenkamercommissie van de gemeente Vaals is er bij de gemeente in Vaals een security scan uitgevoerd. Tijdens dit bezoek is gekeken naar zowel de fysieke als logische beveiliging van het netwerk.

Naar aanleiding hiervan is een rapport opgesteld met de bevindingen, conclusies en aanbevelingen. De bevindingen voor de locatie zijn zeer positief. Het gebouw zelf voldoet aan een hoge mate van beveiliging al is hier toch nog een klein punt waar naar gekeken moet worden. Het fysieke netwerk is netjes afgesloten, de faciliteiten van de server ruimte zijn hierbij niet helemaal voldoende en het logische netwerk zit goed doordacht in elkaar. Het netwerk voldoet dus aan de gestelde eisen.

Op het gebied van remote acces zijn er toch nog een paar punten waarop men moet letten. Het CDP en Telnet protocol zijn voor gebruikers niet uitgeschakeld, hierdoor kan een user toegang krijgen tot een router. Verder wordt er nog geen gebruik gemaakt van een intrusion detection/prevention system bij de toegang van en naar het Internet.

Het netwerk zelf is opgebouwd uit een Windows 2003 server omgeving welke nagenoeg goed in elkaar zit. De shares structuur die momenteel wordt toegepast is achterhaald en men heeft dan ook vermeld dat dit wordt aangepast. De huidige structuur is goed en doordacht, wij willen dan ook meegegeven dit bij de nieuwe structuur te doen.

2. Inleiding

In het kader van het rekenkameronderzoek naar dossiervorming is NID Solutions gevraagd om een security scan uit te voeren op de locatie gemeente Vaals. De gemeente Vaals heeft ongeveer 80 werknemers in dienst die gebruik maken van het netwerk, twee van deze personen beheren en onderhouden het netwerk. De rekenkamercommissie wil graag weten of de digitale infrastructuur capabel is om te kunnen faciliteren bij een digitalisering van de informatiestromen binnen het gemeentebedrijf.

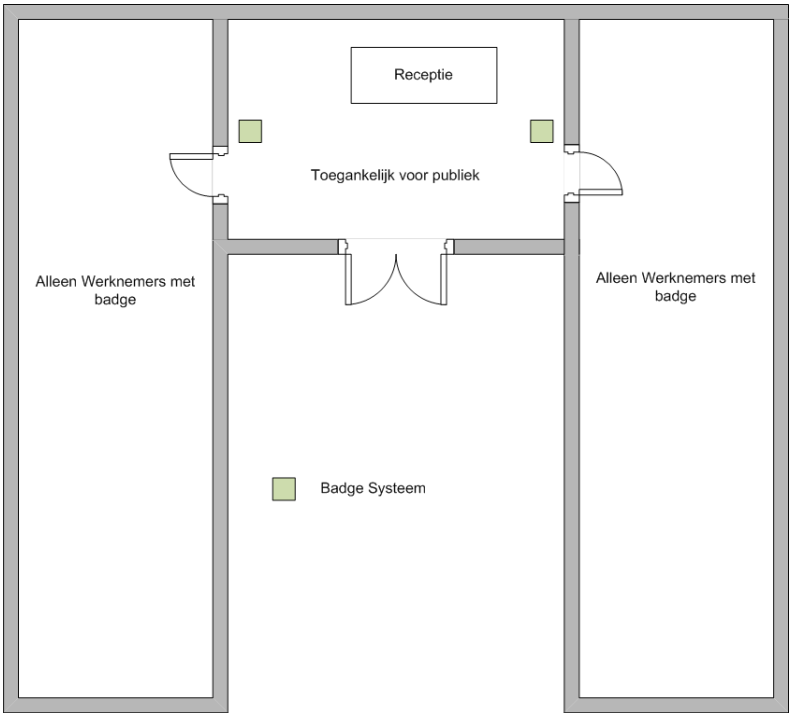
De opdracht luidt als volgt, het gehele netwerk mag aan een onderzoek onderworpen worden op het gebied van security breuken met als uitzondering het GBA systeem. Het is de bedoeling dat de NID studenten op het gebied van security een aantal zaken gaan onderzoeken. Zowel de beveiliging betreffende de toegang tot het gebouw en of bepaalde ruimten moeten worden onderzocht, tevens moet het netwerk van de gemeente Vaals onderworpen worden aan een security scan.

Het netwerk van de gemeente Vaals is opgebouwd uit een Windows 2003 server omgeving. De gebruikers in het netwerk maken gebruik van het Windows XP of 2000 Operating System en zijn aangesloten op het netwerk via een ster topologie.

In dit adviesrapport wordt uitgelegd op welke punten er onderzoek is gepleegd en welke resultaten dit heeft opgeleverd. Zowel positieve als negatieve security aspecten zullen aan het licht komen en nader worden beargumenteerd.

3. Building Security

Het gebouw waar de gemeente Vaals gebruik van maakt is op bepaalde tijden toegankelijk voor het publiek. Deze personen worden aan de receptie ontvangen en kunnen geen verdere toegang krijgen tot het pand. Het pand is beveiligd met een badge systeem, dat wil zeggen dat alle medewerkers van de gemeente Vaals een badge hebben gekregen waarmee zei toegang tot het pand kunnen krijgen. Hieronder wordt in een tekening aangegeven hoe het gebouw eruit ziet en in welke mate werknemers en het publiek toegang hebben tot het pand.



Het kan natuurlijk voorkomen dat een persoon een afspraak heeft met een werknemer van de gemeente, deze persoon kan dan onder begeleiding van de werknemer toegang krijgen tot het beveiligde gedeelte, het is normaler wijs uitgesloten dat niet geautoriseerde personen toegang krijgen.

Dit badge systeem werkt goed, er is dan ook geen noodzaak om hier een verandering in aan te brengen. Naast de hoofdingang zijn er aan de zijkant van het gebouw ook nog verscheidene ingangen, deze worden door werknemers gebruikt om af en toe te roken of als uitgang. Op deze ingangen is geen controle, dit is dus een punt waar men aandacht aan moet besteden.

4. Perimeter security

De gemeente Vaals heeft een verbinding met het Internet die aangeboden wordt door Essent. Het betreft hier een rechtstreekse verbinding met het Internet doormiddel van een @Work abonnement.

Omdat een Internet verbinding altijd een groot risico voor de veiligheid van een netwerk kan betekenen is het zaak deze verbinding te beschermen tegen misbruik. Hier is door de gemeente goed over nagedacht: de koppeling met het Internet verloopt via een Juniper Netscreen firewall.

Het enige wat hierover op te merken valt is dat de firewall geen ondersteuning biedt voor de laatste mogelijkheden op het gebied van intrusion detection of zelfs intrusion prevention. Dit houdt een verder gaande inspectie van het dataverkeer in op data packet niveau, wat weer een hogere mate van veiligheid oplevert.

Wel moet hierbij vermeld worden dat dit risico een veel grotere impact heeft op het netwerk, wanneer er op grotere schaal gebruik gemaakt wordt van diensten, die aan het Internet geleverd worden. Hierbij denken we aan zaken zoals een web- of mailserver.

In deze situatie zou dan ook ons advies zijn om te upgraden naar een firewall met een uitgebreider pakket aan mogelijkheden, voornamelijk betreffende intrusion detection/prevention systemen.

5. Remote Access Security

Tijdens ons onderzoek kwam één aspect betreffende remote-access aan het licht. Het handelt zich hier om een Cisco 801 ISDN router die hoogstwaarschijnlijk door GBA gebruikt wordt om op afstand toegang te krijgen tot hun systeem. In de volgende twee secties zullen we de veiligheid kwesties van deze router belichten.

Op de router staat CDP ingeschakeld. CDP is een Cisco protocol dat ervoor zorgt dat Cisco apparatuur onderling informatie kan uitwisselen over layer 2, aldoende een beter inzicht in het netwerk te krijgen. Dit protocol hoort echter normaal richting de gebruikers en openbare netwerken uitgeschakeld te zijn. Een simpele 2 minuten log van het netwerkverkeer geeft al duidelijk het serienummer en versienummer van deze router prijs op packet niveau. Dit houdt in dat er voor eventuele kwaadwillende gericht gezocht zou kunnen worden naar bekende fouten in deze versie van IOS. Als er voor de gebruikte versie een exploit te vinden is, kan de gebruiker zich op deze manier toegang verschaffen tot de configuratie console van de router en zo externe toegang regelen. Ons advies is dan ook om CDP uit te schakelen op de router.

Een andere configuratie die op deze router aangepast zou kunnen worden om de security positief te beïnvloeden, is het uitschakelen van Telnet. Telnet is een onveilig protocol omdat het gegevens zonder enige vorm van encryptie over het netwerk verstuurd. Het verbeteren van deze veiligheid is echter geen grote klus. Met een kleine configuratie wijziging is het mogelijk om de router gebruik te laten maken van SSH, wat wel gebruik maakt van een beveiligde verbinding.

Verdere vormen van remote access zijn ons onbekend gebleven en zijn daarom niet behandeld.

6. Central site – Access Control Security

De server hardware van de gemeente Vaals bevindt zich op de eerste verdieping. De hardware is opgezet in een afsluitbare ruimte waar alleen IT personeel toegang toe kan krijgen middels een sleutel. De ruimte voldoet niet aan alle eisen die aan een serverruimte worden gesteld. De volgende punten zijn opgemerkt tijdens de survey.

- Er is geen brandwerende deur aanwezig;
- Er is geen verhoogde vloer en verlaagd plafond aanwezig;
- Er is een raam aanwezig in de ruimte.

De punten die hierboven zijn opgenoemd zijn toch van groot belang, een server ruimte is een ruimte waar veel gebeurd qua warmte en elektra en water. Zaken als een lekkende airconditioning of iemand die bijvoorbeeld een steen door een raam naar binnen gooit, kan een groot heikel punt worden.

Verder is er een opmerking betreffende de patchkast, dit is op het moment een grootte wirwar van draden. Om een goed overzicht te houden en natuurlijk ook niet de verkeerde stekker uit te trekken raden wij aan om de patchkast opnieuw te bedraden, wellicht met een hogere klasse bekabeling om breuken door doorhangen te voorkomen.

6.1.Environmental/Electrical Security

Bij de gemeente Vaals is het wenselijk dat de omgeving altijd up-and-running is. Om dit te realiseren zullen er in de serverruimte een aantal zaken geregeld moeten zijn. Hieronder is in een tabel te zien welke eisen er aan een serverruimte worden gesteld. Hieruit kan worden opgemaakt of er zaken aanwezig zijn op de gemeente Vaals of niet.

Componenten	*Aanwezig*	*Opmerking*
Verhoogde deur		Niet aanwezig in de ruimte
Brandveilige deur		De ruimte is voorzien van een houten deur
Gesloten ruimte		Er bevindt zich een raam in de ruimte
Airconditioning	V	De plaatsing kan beter. De airconditioning hangt momenteel boven de servers
Branddeken	V	De plaatsing kan beter buiten de serverruimte
UPS	V	
Brandblusser	V	
Brandalarm	V	
Vochtigheidsalarm	V	
Afsluitbare deur	V	
Patchkast	V	Deze moet opnieuw geordend worden

Al met al zijn er toch nog een aantal punten die in de toekomst verholpen kunnen worden. De kans is vrij groot dat er calamiteiten veroorzaakt kunnen worden als de serverruimte niet voldoet aan de eisen. Een verhoogde vloer, brandveilige deur en het raam dat zich in de ruimte bevind zijn zaken die zeker aandacht nodig hebben.

7. Data Security

De huidige shares structuur, die berust op een Windows 2003 domain, is verdeeld op basis van afdelingen en type van de documenten. Per afdeling wordt er doormiddel van een Group bepaald wat er op deze map uitgevoerd mag worden. Ondanks het zich toch om een groot aantal mappen handelt, hebben wij moeten constateren dat deze rechten overal zorgvuldig zijn toegekend waardoor hier in ieder geval geen directe problemen door zouden moeten ontstaan.

Wel hebben wij moeten constateren dat er geen gebruik gemaakt wordt van de auditing functies die Windows Server 2003 biedt voor deze shares. Het configureren van een Log on Failure of zelf Log on Success and Log on failure biedt een zeer compleet overzicht wanneer gebruikers pogingen doen om aan data te komen. Het grote voordeel van de Log on Success instelling is de mogelijkheid tot inzien van gebruik wanneer er bijvoorbeeld een document verloren gaat of gewijzigd wordt op een onjuiste manier en men wil weten wie deze problematiek veroorzaakt.

We hebben echter mogen vernemen dat het huidige ontwerp verouderd is en er gewerkt wordt aan een nieuwe omgeving. Ons advies is om hierbij net zo zorgvuldig om te gaan met het instellen van de rechten zoals dit al gebeurd is en om toch na te denken over een auditing policy over de shares.

8. Security Management

Het is belangrijk om te kunnen detecteren en monitoren van vreemde acties welke van het Internet afkomstig zijn. Momenteel is er een Netscreen firewall aanwezig. Een dergelijke firewall heeft een ondersteuning voor SNMP. Met dit protocol kan informatie van de firewall worden doorgestuurd naar een applicatie die bijvoorbeeld op een server draait. Deze applicatie kan eventueel een actie ondernemen bij een bepaalde constatering op de firewall.

De beheerders hebben aangegeven dat er de mogelijkheid is om een USB stick te gebruiken op lokale computers. Dit is uiteraard een groot security issue. Een gebruiker kan op deze manier data opslaan en zo via een andere weg, buiten de gemeente om, verspreiden. Het is echter moeilijk om USB geheel uit te schakelen in verband met andere hardware als een muis ook met USB werkt.

Als een USB stick wordt gebruikt, krijgt deze normaliter “F” als schijfletter. Dezelfde schijfletter wordt echter gebruikt voor een share naar de fileserver. Dit verhinderd voor veel gebruikers al het gebruik van een USB stick, het is echter met 2 a 3 muisklikken te omzeilen. Een mogelijkheid is om het gebruik van USB sticks te verbieden in een overkomst en/of policy voor het gebruik van de computersystemen.

9. Policy Security

Gebruikers die inloggen op een computersysteem hebben lokaal op het systeem geen administrator rechten. Dit betekend dat het in de meeste gevallen onmogelijk is om applicaties te installeren of te verwijderen.

Binnen de Active directory wordt voornamelijk gewerkt met één security policy. De “default domain policy” is verwijderd op domein niveau en op elke onderliggende OU is een zelf gemaakte policy geplaatst: First policy.

Binnen deze policy worden alle mogelijke zaken gedefinieerd. Hierbinnen wordt gedefinieerd dat gebruikers wachtwoord elke 49 dagen gewijzigd wordt, waarbij de laatste 24 wachtwoorden bewaard blijven. Een wachtwoord moet 5 karakters lang zijn in deze policy. Dit is een punt van aandacht. Het is vrij gebruikelijk binnen een dergelijke omgeving om minimaal 7 karakters te gebruiken voor het wachtwoord, dit verkleint meteen de kans op het achterhalen van een wachtwoord.

Na een scan van de domain controller server zijn de volgende punten naar voren gekomen:
- Updates worden automatisch gedownload maar niet geïnstalleerd
- Er zijn enkele standaard applicaties aanwezig die niet noodzakelijk zijn
- SA account van SQL server heeft geen/onveilig wachtwoord
- Geen mixed mode authenticatie voor SQL

Er is tevens een zelfde soort scan uitgevoerd op de Microsoft Exchange server:
- Er missen enkele security updates
- Geen service pack geïnstalleerd voor SQL server

Windows Updates zijn belangrijk voor het veilig houden van een netwerk omgeving. Bij het missen van updates en/of security packs kunnen er mogelijkheden zijn om niet gewenste zaken uit te voeren. Het is een noodzaak om updates/service packs eerst uit te testen in een test omgeving alvorens deze daadwerkelijk geïnstalleerd worden. Dit dient wel spoedig te gebeuren na het uitkomen van de updates zodat deze snel en correct op de servers en werkstations geïnstalleerd kunnen worden om zo enige veiligheid te garanderen.

10.Social Engineering

Social engineering is in deze situatie lastig te onderzoeken, zeker als verschillende mensen weten van dit onderzoek. Opvallend was echter dat wij vrij gemakkelijk een administrator wachtwoord hebben gekregen zonder verdere voorwaarden. Dit is echter niet representatief aangezien wij met dit onderzoek bezig zijn.

11.Conclusie

Het netwerk heeft een redelijke hoge mate van veiligheid, echter enkele punten missen om een perfecte omgeving te krijgen. Hieronder een opsomming van de kwesties die wij zijn tegengekomen in ons onderzoek:

- Serverruimte
  - geen brandwerende deur
  - aanwezigheid van een raam
  - verkeerde locatie van de branddeken
  - geen verhoogde vloer
  - chaotische Patchkast
- Domain controller/exchange server
  - missende security updates
  - missend service pack
  - geen auditing
- Social engineering
  - vrij eenvoudig administrator wachtwoord achterhaald zonder voorwaarden
- Access securtity
  - iedereen kan mbv pc of notebook toegang krijgen tot het netwerk
  - het is eenvoudig het gehele netwerk af te luisteren vanaf één poort door de afwezigheid van een MAC limit of link.
- Building Security
  - De deuren aan de zijkanten van het gebouw zijn onbewaakt en worden niet gecontroleerd.

Dit resulteert in onderstaande adviezen:

- Aanpassing of verplaatsing van de serverruimte naar een plaats die voldoet aan de bovengenoemde punten
- Een duidelijke procedure opstellen voor het updaten en onderhouden van de servers en werkstations, eventueel met een (virtuele) testomgeving waar patches uitgetest kunnen worden alvorens een werkelijke implementatie
- Auditing configuren op de servers om zodoende achteraf te kunnen achterhalen wie, wat, waar en wanneer gedaan heeft
- Een MAC filtering toepassen op de switches zodat onbekende computers en notebooks geen toegang krijgen tot het netwerk en het gebruiken van een MAC attack niet lijdt tot afluisterbaarheid van het algehele verkeer.
- Medewerkers (wederom) attenderen op de deuren aan de zijkanten van het gebouw, zodat deze nooit onbewaakt geopend blijven.

Antwoord gevende op de opdrachtformulering: "Is de digitale infrastructuur capabel om te kunnen faciliteren bij een digitalisering van de informatiestromen binnen het gemeentebedrijf?", kunnen we concluderen dat de complete infrastructuur momenteel geschikt is voor huidige informatiestromen. Kijkende naar toekomstige informatiestromen en eisen dan dienen bovenstaande adviezen (grotendeels) aangenomen worden en de omgeving aangepast worden met de genoemde punten. Uiteindelijk kunnen we concluderen dat de algemene beveiliging van het netwerk goed in elkaar zit. Er is veel aandacht naar uit gegaan vanuit de beheerafdeling.