Praktische handleiding voor het veilige gebruik van elektronische certificaten in de medische context

eHealth Réf : mibr/V1/V1/2012.E.068/Certificates.UserGuideLines/NL/1.0.

Versie	Status	Datum	Auteur(s)	Aard van de wijzigingen
1.0	Final	10/09/2012	eHealth	

Inhoudsopgave

1. Inleiding

Om de gegevensuitwisseling in de medische sector te beveiligen en te verhinderen dat de gegevens onderschept zouden worden door onbevoegden worden er gesofisticeerde veiligheidsmechanismen geïmplementeerd.

Daartoe wordt in het kader van deze veiligheidsmaatregelen een beroep gedaan op de vercijferingsprincipes met gebruik van asymmetrische vercijfering en sleutelparen (private sleutel / publieke sleutel)[1].

1.1. Scope

De bedoeling van dit document is om een aantal aanbevelingen inzake veiligheid te formuleren met betrekking tot het gebruik van het certificaat en de bijbehorende sleutels aan de hand waarvan toegang kan worden verkregen tot vertrouwelijke gegevens.

Naast de hierna vermelde veiligheidsaanbevelingen bevat dit document aangaande het gebruik van de certificaten en sleutels ook algemene aanbevelingen inzake veiligheid om te vermijden dat een incident een rechtstreekse of onrechtstreekse impact zou hebben.

Voor een goed begrip van de principes van de certificaten en van de bijbehorende sleutels, vermeldt de auteur een aantal artikelen die hierop betrekking hebben:

- http://en.wikipedia.org/wiki/Public_key_certificate (EN) ;
- http://fr.wikipedia.org/wiki/Certificat_%C3%A9lectronique (FR)
- http://nl.wikipedia.org/wiki/Certificaat_%28PKI%29 (NL)
- http://www.pgpi.org/doc/pgpintro/ (EN)
- http://technet.microsoft.com/en-gb/library/aa998077%28v=exchg.65%29.aspx?wt.svl=2007resources+%3b (EN)
- http://technet.microsoft.com/fr-fr/library/aa998077%28EXCHG.65%29.aspx?wt.svl=2007resources%20; (FR)
- https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Certificate_System/8.0/html/Deployment_Guide/Introduction_to_Public_Key_Cryptography.html (EN)
- http://www.cairn.info/revue-les-cahiers-du-numerique-2003-3-page-101.htm (FR)
- http://www.commentcamarche.net/contents/crypto/certificat.php3 ; (FR)

1.2. Voorstelling

De eHealth-certificaten worden gebruikt om tegemoet te komen aan twee behoeften:

- de authenticatie van de actoren van de gezondheidszorg,
- als basis voor de aanmaak van de dubbele vercijferingssleutel (ETK) die gebruikt wordt door de vercijferingsdienst.

Wanneer een zorgverlener toegang wenst tot bepaalde basisdiensten van het eHealth-platform met gebruik van een system-to-systemverbinding en niet een webtoepassing, moet hij over een eHealth-certificaat beschikken. De “systeem”-partner wordt aan de hand van dit certificaat geïdentificeerd en geauthentiseerd, terwijl de gebruiker (persoon) op basis van de eID of de burgertoken geïdentificeerd en geauthentiseerd wordt.

Dit geldt zowel voor het gebruik van basisdiensten als voor het gebruik van diensten met toegevoegde waarde die aangeboden worden in de vorm van webservices. De software-integratoren (niet de zorgverleners) kunnen bovendien test-certificaten aanvragen. Op basis van deze certificaten kunnen de IT-medewerkers van deze

[1]De vercijfering met gebruik van een symmetrische sleutel wordt uitgelegd in 5 Bijlage, onder punt 5.1.

software-integratoren, die actief zijn in de Belgische gezondheidszorg, de integratie van onze basisdiensten testen.

Het eHealth-authenticatiecertificaat is een bestand dat alle nodige informatie bevat om de verzender te identificeren. Het certificaat is een officiële verklaring, ondertekend door een betrouwbare autoriteit die bevoegd is om de relatie tussen de elektronische publieke sleutel en de identiteit van de titularis te certificeren. Het eHealth-certificaat wordt door dezelfde certificatie-autoriteit gecertificeerd als de elektronische identiteitskaart (CA root : Fedict, operationele CA : Certipost).

Elke zorgverlener zal als entiteit de eHealth-certificaten kunnen gebruiken. Het eHealth-authenticatiecertificaat certificeert hetzij de identiteit van natuurlijke personen die gekend zijn in de authentieke bron "kadaster van de gezondheidszorgberoepen", hetzij de identiteit van instellingen die actief zijn in de sector van de Belgische gezondheidszorg. Voor actoren die geen medisch beroep uitoefenen maar die ook actief zijn in de sector van de Belgische gezondheidszorg (zoals softwarebedrijven) bestaat er een officieel eHealth-testcertificaat aan de hand waarvan toepassingen kunnen worden getest zonder dat medische gegevens worden onthuld.

Indien de instelling dit wenst, kan ze verschillende certificaten krijgen voor eenzelfde entiteit met de bedoeling de toepassingen van elkaar te scheiden of de productieomgeving van de testomgeving te scheiden.

2. Principes van identificatie, authenticatie en handtekening binnen het -eHealth-platform[2]

Voor de implementatie van een toepassing voor de sector van de gezondheidszorg, bijvoorbeeld (My)CareNet of Recip-e, heeft het eHealth-platform een document op zijn portaal gepubliceerd waarin de principes van identificatie, authenticatie en handtekening worden uitgelegd.

Elke toepassing die gebruik wil maken van een elektronische dienst van het eHealth-platform, van (My)CareNet of Recip-e dient zich te authentiseren aan de hand van een private sleutel en het bijbehorende authenticatiecertificaat uitgereikt door het eHealth-platform.

Het authenticatiecertificaat van de toepassing bevat de identiteit van de verantwoordelijke voor het beheer van de toepassing. Het eHealth-platform heeft duidelijke instructies uitgewerkt met betrekking tot het verkrijgen en installeren van dit authenticatiecertificaat. De installatie en het beheer van dit authenticatiecertificaat is de bevoegdheid van de verantwoordelijke voor het beheer van de toepassing.

De basisdienst "gebruikers- en toegangsbeheer" van het eHealth-platform laat toe na te gaan of een bepaalde gebruiker van een elektronische dienst van het eHealth-platform, van (My)CareNet of Recip-e bepaalde kenmerken of relaties bezit; indien niet, wordt er een foutbericht gegenereerd. Het eHealth-platform controleert niet of een bepaalde gebruiker een bepaalde lokale toepassing mag gebruiken. Gelet op het soort gegevens dat door deze lokale toepassingen wordt verwerkt, wordt het gebruik van een sterke authenticatie (eID, SmartCard, Secure Token) aanbevolen.

[2] Cf. website van het eHealth-platform: https://www.ehealth.fgov.be/nl/registratie-van-de-medische-softwarepakketten, Recip-e: Mechanismen ter identificatie, authenticatie en ondertekening

3. Algemene principes inzake certificaten

3.1. eHealth-certificaten

De uitwisseling van informatie en het tot stand brengen van een connectie met het eHealth-platform vereist de implementatie van een certificaat en de bijbehorende sleutels. Het eHealth-platform heeft een procedure en een utiliteitsprogramma (ETK) uitgewerkt voor de indiening van de aanvraag. De certificaten laten niet alleen de identificatie / authenticatie toe, maar ook de vercijfering aan de hand van publieke / private sleutels.

Op basis van het eHealth-certificaat kan de entiteit zich identificeren en authentiseren in het kader van de uitwisselingen met haar partners. Bovendien waarborgt het ook de onweerlegbaarheid van alle transacties / handelingen die via dit certificaat ondertekend worden.

Het gebruik van het publiek / privaat sleutelpaar laat de vercijfering en ontcijfering (encryptie en decryptie) toe die nodig zijn voor de uitwisseling van "vertrouwelijke" berichten tussen partners binnen de sector van de gezondheidszorg.

Het eHealth-platform laat elke entiteit vrij om al dan niet meerdere certificaten te bestellen en te gebruiken in functie van de professionele activiteit. Bijvoorbeeld: persoonlijk certificaat, certificaat van de instelling, ...

De certificaten die uitgereikt worden door het eHealth-platform zijn eigendom van de aanvrager ervan. Elke uitwisseling en mededeling gebeurt uitsluitend onder de verantwoordelijkheid van deze laatste.

3.2. Beheer van de paswoorden

Om het gebruik en dus de toegang tot de private sleutel van een certificaat te beveiligen, wordt gebruik gemaakt van een authenticatiemechanisme gebaseerd op de invoering van een toegangscode (paswoord, pincode, ...). Deze werkwijze wordt ook toegepast in het kader van de opslagruimte voor de certificaten en bijbehorende sleutels.

Het efficiënte beheer van de paswoorden is de belangrijkste hoeksteen van de elektronische beveiliging van een organisatie. Bij gebruik van elektronische tools waarbij een authenticatie noodzakelijk of zelfs verplicht is, wordt meestal gebruik gemaakt van een toegangscode (pincode, paswoord, e.d.). Het is dan ook niet uitzonderlijk dat een gebruiker over een veelvoud van dergelijke identiteitsbewijzen beschikt.

Bijvoorbeeld :

- de pincode voor de Belgische elektronische identiteitskaart,
- de pincode van de betaalkaart,
- een paswoord voor de computer,
- toegangscodes voor toepassingen, zowel voor professioneel als privé-gebruik,
- ...

De gebruiker dient dus een heleboel van dergelijke codes te onthouden en is daarom geneigd om uit gemak éénzelfde toegangscode of een gemakkelijk te onthouden code te gebruiken, om de codes ergens op te schrijven en in de nabijheid te bewaren (onder het toetsenbord, in de eerste lade van het bureau, ...). Dit heeft een invloed op het veiligheidsniveau van de gegevens / toepassingen die door deze codes beveiligd worden.

Het paswoord moet gemakkelijk te onthouden zijn maar tegelijkertijd voldoende complex om niet achterhaald te worden. De goede praktijken bevelen het volgende aan:

- het paswoord mag niet hetzelfde zijn als de naam van de gebruiker, ook niet met toevoeging van een cijfer of symbool;
- het paswoord mag geen persoonlijke informatie bevatten, zoals een straatnaam of huisnummer, de bedrijfsnaam, de geboortedatum, enz.;

- het paswoord mag nooit namen van familieleden, huisdieren, vrienden of collega's bevatten;
- het paswoord mag geen bekende zinsnede zijn gevolgd door een cijfer dat verandert wanneer het paswoord vervalt;
- een paswoord dat gebruikt wordt in het kader van een bepaald doeleinde mag niet voor andere doeleinden worden gebruikt;
    - het paswoord mag enkel worden gebruikt in het kader van een bepaalde toegang;
    - een paswoord dat gebruikt wordt voor de aanmaak van een private sleutel mag niet meer worden gebruikt voor de aanmaak van andere private sleutels;
    - ...

Paswoord	Sterkte	Reden
Wind	Zwak	Te kort, gemakkelijk te achterhalen / raden.
Laurent1	Zwak	Gebruik van de voornaam van de gebruiker, te eenvoudig.
2265	Zwak	Zelfde code als pincode van bankkaart van de gebruiker. Bovendien brengt dit risico's mee voor het gebruik van de bankkaart.
Hzc4uG	Goed	Zes karakters, hoofdletters en kleine letters en een cijfer.
3zX2tRk4c+y	Zeer goed	Paswoord gegenereerd door het systeem.

Tabel 1 : Voorbeelden sterkte van paswoorden

Er bestaan verschillende manieren om een paswoord te creëren dat voldoende sterk is om niet achterhaald te worden en dat toch gemakkelijk kan worden onthouden. De meest gebruikte werkwijze bestaat erin een zin te maken die voldoende lang is en tegelijkertijd gemakkelijk te onthouden en daarop een proces van selectie van karakters toe te passen die een paswoord vormen. Het aldus gevormde paswoord wordt een "passphrase" genoemd.

Voorbeeld:

> Vertrekkend vanuit de volgende zin: " Bob wil een geheime sleutel delen met zijn collega Alice!", is het mogelijk om een passphrase te genereren met zowel kleine letters als hoofdletters, maar ook cijfers en andere speciale karakters. Op basis van de vorige zin kan ook een paswoord worden gecreëerd zoals: " Bw1gSdMzC@!".

Niet alleen de keuze van het paswoord is belangrijk, ook de opslag ervan. Een paswoord is per definitie geheim en moet dat ook blijven. Dit paswoord in de buurt van het scherm bewaren, onder het toetsenbord of in de eerste lade van het bureau is dus helemaal geen goed idee!

Aangezien het paswoord gebruikt wordt voor de identificatie en authenticatie en soms ook voor het plaatsen van een handtekening mag het enkel worden meegedeeld met het oog op preventie om belangrijke potentiële problemen te vermijden. De verantwoordelijkheid voor het gebruik van dit paswoord berust bij de eigenaar ervan.

Zelfs met inachtneming van alle veiligheidsmaatregelen blijft de betrouwbaarheid van een paswoord niet gewaarborgd doorheen de tijd, daarom is het belangrijk om dit paswoord regelmatig te wijzigen.

> *In het kader van het ETEE-project, stelt het eHealth-platform een tool ter beschikking om paswoorden te wijzigen. Deze tool is beschikbaar op het portaal[3].*

3.3. Keystore[4]

Zoals beschreven in het hoofdstuk "Definities" is de keystore of sleuteldepot een opslagruimte voor alle publieke en private sleutels die in gebruik zijn. Het veiligheidsniveau verdient dan ook bijzondere aandacht. Het betreft daarbij zowel de toegankelijkheid, de duurzaamheid en de onweerlegbaarheid.

[3] https://www.ehealth.fgov.be/nl/application/applications/beheer_ehealth_certificaten.html

[4] Definitie van Keystore zie punt5.1 pagina 18

Om de vertrouwelijkheid van de sleutels te garanderen is deze opslagruimte enkel toegankelijk voor de gemachtigde gebruikers. De toegangsrechten dienen beschreven te worden in de documenten waarin de implementatie van de veiligheid binnen de entiteit uitgelegd wordt. Deze documenten worden "security policy's" genoemd.

Elke schending van het informatiesysteem en dus potentieel van de inhoud van de keystore heeft tot gevolg dat de vertrouwelijkheid van de certificaten en bijbehorende sleutels aangetast is, waardoor het gebruik ervan in het kader van de uitwisseling en de toegang tot "gevoelige" gegevens niet meer mogelijk is. Bijgevolg zal een procedure van herroeping van de certificaten en bijbehorende sleutels opgestart worden. Echter, in geval van een fysiek incident met betrekking tot dit informatiesysteem is het mogelijk om een beveiligde back-up van deze opslagruimte te realiseren[5] om het systeem en de toegang ertoe te herstellen.

De traceerbaarheid van de acties die verricht worden op de keystore wordt verzekerd door de implementatie van een intern auditsysteem binnen het exploitatiesysteem. Deze auditing laat toe om via de systeemloggings na te gaan welke acties gerealiseerd werden door alle gebruikers die toegang hebben gehad.

Deze drie punten dienen te worden beschreven in een document met betrekking tot de veiligheidsmaatregelen die binnen de organisatie werden getroffen.

3.4. Beveiliging van de private sleutel

Tenzij voor backupdoeleinden, zoals hierboven beschreven voor wat de keystore betreft, is het niet aanbevolen om een kopie van de private sleutel te nemen.

Gelet op de functionaliteiten van de private sleutel, dienen zowel de procedure van back-up of archivering als de opslagruimte en de lokalisatie ervan beveiligd en beschermd te worden.

De vernietiging van de sleutels en certificaten mag enkel gebeuren door een bevoegde persoon binnen de entiteit. Deze procedure moet bovendien worden opgenomen in de algemene veiligheidsdocumenten (veiligheidsbeleid, veiligheidsplan, ...).

Om oudere vercijferde berichten opnieuw te raadplegen[6] na het verstrijken van de periode van geldigheid van het certificaat is de implementatie van een back-up via de organisatie van een archiveringsprocedure vereist.

3.5. Beheer van de certificaten

De certificaten uitgereikt door het eHealth-platform hebben een geldigheidsduur van maximum 3 jaar. Het eHealth-platform zal de betrokkene per e-mail[7] verwittigen vanaf 3 maanden voor het verstrijken van het certificaat.

Op het portaal van het eHealth-platform is een procedure beschikbaar om een mandaat toe te kennen aan een derde voor het bestellen en beheren van certificaten uitgereikt door het eHealth-platform.

Gelet op het verband tussen de authenticatie- en vercijferingscertificaten is de hernieuwingsprocedure automatisch van toepassing voor beide.

Eenmaal de vervaldatum van het certificaat verstreken is, zal het niet meer gebruikt kunnen worden. Om problemen te vermijden als gevolg van het verstrijken van de geldigheidsduur van het certificaat, wordt een termijn van 3 maanden voorzien voor de hernieuwingsaanvraag.

Om vercijferde berichten opnieuw te kunnen raadplegen na het verstrijken van de geldigheid van het certificaat is het aanbevolen om een beveiligde archivering van de keystore en de bijbehorende paswoorden te organiseren 6.

[5] Beveiligde back-up: fysiek gescheiden opslagruimte met een veiligheidsniveau dat minstens even hoog is als het veiligheidsniveau van de keystore.

[6] Bij het opstellen van dit document biedt het eHealth-platform een oplossing voor de uitwisseling van vercijferde berichten maar nog geen oplossing voor de opslag van deze vercijferde berichten op lange termijn.

[7] Op het e-mail adres dat de gebruiker ingevoerd heeft bij de aanvraag van het certificaat. Een herinnering wordt maandelijks verstuurd, vanaf 3 maand voor vervaldatum en zolang het certificaat niet vernieuwd werd.

De namaak van eHealth-certificaten is verboden. Het zal trouwens niet mogelijk zijn om te communiceren met gebruik van "valse" certificaten gelet op de geldigheidscontroles die worden toegepast en het feit dat de private sleutel niet bekendgemaakt wordt in de publieke ruimte.

Het eHealth-platform heeft een standaardprocedure uitgewerkt zowel voor de aanvraag als voor de hernieuwing en tevens voor de herroeping van het certificaat.[8].

De vraag tot herroeping van het certificaat kan enkel worden ingediend door de aanvrager van het certificaat, diens mandataris, de Verantwoordelijke Toegangen Entiteit (VTE)[9] of, in laatste instantie, door de veiligheidsconsulent van het eHealth-platform. Elke aanvraag tot herroeping dient vergezeld te zijn van een identiteitsbewijs, een elektronische handtekening (eID) of een getekende kopie van de identiteitskaart van de aanvrager.

3.6. Mandaat

Het eHealth-platform heeft op zijn portaal een formulier ter beschikking gesteld waarmee een mandaat kan worden verleend aan een persoon binnen of buiten de entiteit voor het beheer van de certificaten en de bijbehorende sleutels[10].

3.7. Noodprocedure

Om de continuïteit van de activiteiten van de entiteit te waarborgen ingeval de identificatie en authenticatie aan de hand van de elektronische identiteitskaart niet mogelijk is (verloren of gestolen kaart, ...) biedt het eHealth-platform een alternatieve oplossing aan door bij de connectie gebruik te maken van het persoonlijk certificaat (verschillend van het systeemcertificaat voor de identificatie en authenticatie van de toepassing). Deze alternatieve oplossing biedt een lager veiligheidsniveau dan het gebruik van de elektronische identiteitskaart en het gebruik ervan wordt beperkt in de tijd ("fallback session"). De toegelaten maximumduur moet in functie van de doelgroep en van de operationele behoeften binnen de stuurgroep van elk project worden vastgelegd in overleg met het eHealth-platform en na risico-analyse.

In het kader van het project Recip-e werd er een noodprocedure afgesproken dat:

- voor de voorschrijvers, de duur van een sessie beperkt is tot 1 (één) uur alvorens opnieuw een identificatie vereist is;
- voor apothekers is de duur van een sessie beperkt tot 4 (vier) uur.

3.8. Herroeping van het certificaat

Als u geen connectie meer tot stand kan brengen en geen gegevens meer kunt uitwisselen op basis van uw certificaat, moeten uw sleutel en uw certifica(a)t(en) vermoedelijk worden vervangen. Alvorens de certificaten en de bijbehorende sleutels te herroepen, kan een analyse van de evolutie van de toestand u een eerste oplossing bieden.

Bijvoorbeeld:

- Is het bestand met de private sleutel nog steeds aanwezig ? (bestand .P12 of controleer in de handleiding van uw medische software)
- Werd het programma recent gewijzigd door een update ?
- …

Neem contact op met het Contactcenter op het nummer 02-788 51 55 en volg de procedure die u meegedeeld zal worden voor de aanmaak van een nieuwe geheime sleutel.

[8] https://www.ehealth.fgov.be/nl/support/basisdiensten/ehealth-certificaten

[9] Voor de definitie van Verantwoordelijke Toegangen Entiteit (VTE) zie punt5.1 pagina 19

[10] https://www.ehealth.fgov.be/nl/support/basisdiensten/ehealth-certificaten

Het certificaat moet worden herroepen (volgens de procedure die beschreven wordt op de website van het eHealth-platform) en een nieuw certificaat moet worden aangevraagd.

3.9. Veiligheidsprincipes m.b.t. de certificaten in specifieke gevallen

a) Gedeeld gebruik (bijvoorbeeld in een medische wachtpost)

In bepaalde omgevingen zal eenzelfde werkstation dat toegang verleent tot de diensten van het eHealth-platform gedeeld worden door meerdere zorgverleners (bijvoorbeeld: medische praktijk van verschillende artsen, ...). In dat geval dienen een aantal bijkomende regels in acht te worden genomen om een degelijk veiligheidsniveau te garanderen.

De identificatie en authenticatie ten aanzien van een applicatie die toegang verleent tot "gevoelige" gegevens aan de hand van de elektronische identiteitskaart is te verkiezen boven de lokale installatie van een persoonlijk certificaat, zeker in het kader van een gedeeld werkstation. Zoals hierboven vermeld mogen de pincode van een elektronische identiteitskaart en het paswoord van het persoonlijk certificaat niet worden meegedeeld aan een derde.

In het kader van het gebruik van een paswoord gekoppeld aan de private sleutel voor de system-to-systemidentificatie, kan de mededeling van deze laatste enkel gebeuren aan gemachtigde personen volgens een vastgestelde veiligheidsprocedure die gevalideerd werd door de veiligheidsconsulent van de entiteit.

In het kader van het project tot realisatie van het medisch voorschrift is het gebruik van de elektronische identiteitskaart te verkiezen boven de installatie op het werkstation van het persoonlijk certificaat uitgereikt door het eHealth-platform.

Om zich te beschermen tegen het ongewenste gebruik door een derde, zal de gebruiker erop toezien zijn sessie steeds af te sluiten als zijn dienst erop zit.

b) Gebruik in een apotheek

Het gebruik van medische software binnen een apotheek waarbij er een beroep wordt gedaan op elektronische diensten (zoals het elektronische voorschrift, ...) van het eHealth-platform vereist de inachtneming van een aantal regels om een degelijk veiligheidsniveau te garanderen.

Opdat alle gebruikte werkstations van de apotheek toegang zouden kunnen hebben tot de elektronische diensten van het eHealth-platform, dient het authenticatiecertificaat op elk werkstation te worden geïnstalleerd.

Om de private sleutel afdoende te beschermen moet het bijbehorende paswoord voldoende complex zijn en mag het enkel worden meegedeeld aan de personen die gemachtigd zijn om die sleutel te gebruiken.

Indien het certificaat en de bijbehorende sleutels aangemaakt en geïnstalleerd worden door de leverancier van de toepassing, dienen de desbetreffende codes enkel voor die apotheek te gelden.

De veiligheidsconsulent van de farmaceutische groep kan in het kader daarvan zijn diensten aanbieden aan de apotheker.

Elk probleem dient te worden gemeld aan de helpdesk die instaat voor de apotheek in kwestie, aangezien er een risico van corruptie van het certificaat en de bijbehorende sleutels bestaat. In dat geval is een herroeping noodzakelijk.

4. Algemene veiligheidsprincipes

Naast de voormelde punten, die rechtstreeks verband houden met het veiligheidsniveau van de certificaten en bijbehorende sleutels in het kader van de uitwisseling van informatie binnen het netwerk van de gezondheidszorgactoren, kunnen ook andere elementen op het vlak van informatieveiligheid een onrechtstreekse impact hebben op de veiligheid van deze certificaten en sleutels. Deze elementen, waarvan sommige hierna beschreven worden, zouden integraal moeten worden opgenomen in het document inzake informatieveiligheid dat opgesteld wordt binnen de entiteit.

Gelet op de "gevoeligheid" van de gegevens die door de verschillende toepassingen worden gebruikt, is de beveiliging van het werkstation van de gebruiker van fundamenteel belang.

Verschillende gebeurtenissen waarover in de pers bericht werd bewijzen dat het veiligheidsniveau van het werkstation van de eindgebruiker een niet te verwaarlozen impact heeft op de veiligheid van de gegevens die door deze gebruiker worden gebruikt in allerhande toepassingen, zowel lokaal als via internet.

> Een voorbeeld: In juni 2012 werden meer dan 13.000 Belgische bankrekeningen gehackt voor een totale waarde van om en bij de 3 miljoen euro als gevolg van de besmetting van de werkstations door malware die gedownload werd vanaf sociale netwerksites.

De installatie van een veiligheidsprogramma dat permanent geüpdatet wordt (met inbegrip van bestrijding van virussen, trojan horses, ...) op elk werkstation[11] is niet langer een aanbeveling maar een verplichting om de gebruiker en de gegevens waarmee hij (zowel professioneel als privé) werkt te beschermen.

4.1. Besturingssysteem

a) Rechten / autorisaties

Om risico's te vermijden op het vlak van de veiligheid van de gegevens die verwerkt worden en waartoe toegang verkregen wordt aan de hand van het certificaat en de bijbehorende sleutels in het kader van zowel privé- als professioneel gebruik, wordt een fysieke scheiding tussen de privé- en beroepsomgeving aanbevolen.

Het aantal lokale accounts op een werkstation dient te worden beperkt. De voorgeïnstalleerde accounts dienen ook te worden gedeactiveerd.

De invoering van een paswoordenbeleid is tevens noodzakelijk om op die manier het gebruik van sterke paswoorden met een minimumlengte op te leggen. Het gebruik van een historiek van paswoorden en een "account lockout threshold" laat toe om het risico van "brute force attack" te vermijden. Het specifieke beleid inzake paswoorden zal worden vastgesteld in samenspraak met de informatieveiligheidsconsulent.

Het hergebruik van identieke paswoorden op verschillende accounts / platformen wordt afgeraden (bv. paswoord van lokale administrator verschillend van de domain-, databasepaswoorden, ...).

Het werkstation dient zodanig te worden geconfigureerd dat een toegangscode noodzakelijk is om op te starten en na een bepaalde periode van inactiviteit, zodat het niet kan worden gebruikt door een derde zonder medeweten van de gebruiker / eigenaar.

Buiten een speciaal beveiligd systeem (SSO) dient de automatische registratie van paswoorden voor netwerk- en internetconnecties, connecties met toepassingen, ... te worden vermeden.

b) Diensten

Zonder het gebruik van de systemen te blokkeren, dienen de lokale functies van sharing[12] te worden vermeden.

[11] De term "werkstation" verwijst naar elk informaticasysteem dat de verwerking van gegevens aan de hand van toepassingen toelaat (o.a. vaste en draagbare pc's, tablets, smartphones, ...).

[12] “simple file sharing”, “shared folders” en “internet connection sharing”

De mogelijkheden van "universal plug & play" dienen te worden gedeactiveerd om elk niet-gemachtigd gebruik van bijkomende hardware te vermijden.

Alle communicatiekanalen[13] die niet noodzakelijk zijn in het kader van de toegestane activiteiten dienen te worden ontkoppeld.

c) Connecties

De interne firewall dient geactiveerd te zijn. Deze firewall moet permanent geactualiseerd worden en mag niet buiten werking worden gesteld door de gebruiker. Enkel de ports die noodzakelijk zijn voor de beroepsactiviteiten mogen worden opengelaten. Er dient een onderscheid te worden gemaakt tussen de connecties die noodzakelijk zijn voor het interne netwerk en de externe connecties.

Naargelang de behoeften dient te worden voorzien in de mogelijkheid om verschillende profielen aan te maken (VPN op laptops, ...).

4.2. Software extern aan het besturingssysteem

a) Webbrowser

De internetparameters van de webbrowser dienen te worden geconfigureerd om te voorkomen dat via internet malware zou worden geïnstalleerd (functies zoals active content, scripting, ... dienen te worden beperkt).

De webbrowser dient, indien mogelijk alleen, na te gaan of elk numeriek certificaat nog geldig is.

Cookies dienen tot een minimum te worden beperkt.

Het gebruik van een "pop-up windows blocker" wordt aanbevolen.

b) Anti-malware

De software ter bestrijding van malware dient zodanig geconfigureerd te worden dat hij regelmatig en automatisch een volledige check van het systeem uitvoert (alle bestanden, met inbegrip van startupbestanden, bios, boot records).

De functies van real-time controle die binnen de anti-malwaresoftware beschikbaar zijn moeten worden geactiveerd.

Deze software dient regelmatig en automatisch te worden geüpdatet.

c) Andere software

Er dienen adequate maatregelen te worden getroffen om de integriteit van de software te waarborgen en het gebruik van software van onbekende oorsprong te vermijden. Het gebruik van gecertificeerde software is een pluspunt.

In geval van installatie van systemen die in staat zijn om op afstand de controle van het werkstation over te nemen, mag deze overname van de controle enkel gebeuren met de toestemming van de eindgebruiker.

De veiligheidslogbestanden die aangemaakt worden bij het gebruik van de toepassing mogen niet worden gewist. Deze bestanden kunnen van pas komen bij gebruiksmoeilijkheden: instabiliteit van de toepassing, onmogelijkheid om een connectie tot stand te brengen, foutbericht van de toepassing.

Open geen onbekende bestanden die bv. via een verdachte mail worden meegedeeld. Deze bestanden kunnen worden gebruikt om een aanval op het systeem in te zetten.

Sluit niet om het even wat aan op de pc, bijvoorbeeld een USB-stick met bestanden die niet door een anti-virus werden gecontroleerd.

[13] wireless network, firewire, bluetooth, infrared, serial, ...

4.3. Patchbeheer

Wat de frequentie van de installatie van veiligheidsupdates betreft, dient er een evenwicht te worden gevonden tussen de behoeften op het vlak van veiligheid en de operationele doelstellingen. Voor updates die als dringend worden bestempeld door erkende instanties[14] dienen onmiddellijk de gepaste maatregelen te worden getroffen.

4.4. Elektronische mailbox

Tenzij er erkende vercijferingstechnieken worden gebruikt (encryptie) wordt een e-mail niet als erg veilig beschouwd. Het verzonden bericht kan door iemand anders dan de bestemmeling worden gelezen. Het ontvangen bericht kan afkomstig zijn van een persoon die zich uitgeeft voor een andere (bedrog , spoofing) en die vertrouwen wekt door het gebruik van nagemaakte logo's. Bijgevolg mag de gebruiker in een e-mail nooit vertrouwelijke informatie meedelen zoals een paswoord, toegangscode, persoonlijke gegevens, etc.

De meest courante bedreigingen zijn de volgende:

- SPAM ;
- phishing ;
- kettingsbrieven;
- hoaxen ;
- trojaanse paarden ;

[14] Sans, Secunia, ….

5. Bijlage

5.1. Definities

Authenticatie

Dit is de controle van de identiteit die de entiteit beweert te bezitten en op basis waarvan die entiteit een elektronische dienst wenst te gebruiken.

De authenticatie vereist een identiteitsbewijs. De controle kan gebeuren op basis van de volgende elementen:

- kennis waarover de gebruiker beschikt (een paswoord, ...);
- bezit (vb. een certificaat op een elektronisch leesbare kaart);
- biometrische kenmerken (handafdruk, ...);
- of een combinatie van verschillende elementen.

Certificaat

Een openbare-sleutelcertificaat wordt meestal kortweg certificaat genoemd. Dit is een digitaal ondertekende verklaring waardoor de waarde van een openbare sleutel wordt gekoppeld aan de identiteit van de persoon, het apparaat of de service met de bijbehorende persoonlijke sleutel. Veel gangbare certificaten zijn gebaseerd op de certificaatstandaard X.509v3.

Certificaten kunnen voor diverse doeleinden worden uitgegeven, bijvoorbeeld voor verificatie van webgebruikers, verificatie van webservers, beveiligde e-mail (S/MIME (Secure/Multipurpose Internet Mail Extensions)), IP-beveiliging (IPSec, Internet Protocol Security), TLS (Transport Layer Security) en handtekeningen bij programmacode. Een certificeringsinstantie (CA) geeft ook certificaten uit aan andere certificeringsinstanties. Zo ontstaat er een certificeringshiërarchie.

De entiteit die het certificaat ontvangt, is de *houder* van het certificaat. De certificeringsinstantie is de uitgever en ondertekenaar van het certificaat.

Certificaten bevatten gewoonlijk de volgende gegevens:

- De waarde van de openbare sleutel van de certificaathouder.
- De identificatiegegevens van de certificaathouder, zoals de naam en het e-mailadres.
- De geldigheidsduur (de periode dat het certificaat geldig is).
- De identificatiegegevens van de uitgever.
- De digitale handtekening van de uitgever. Deze handtekening bekrachtigt de geldigheid van de relatie tussen de openbare sleutel en de identificatiegegevens van de certificaathouder.

De geldigheid van een certificaat is beperkt tot de tijdsperiode die in het certificaat wordt vermeld. Elk certificaat bevat de datums *Geldig van* en *Geldig tot.* Wanneer de geldigheidsperiode van een certificaat is verstreken, moet de houder van het op dat moment verlopen certificaat een nieuw certificaat aanvragen.

In bepaalde gevallen kan het nodig zijn om de relatie die in een certificaat wordt bekrachtigd, ongedaan te maken. Het certificaat wordt dan ingetrokken door de uitgever. Elke uitgever houdt een certificaatintrekkingslijst bij. Aan de hand van deze lijst kan de geldigheid van een certificaat worden gecontroleerd.

Een van de belangrijkste voordelen van certificaten is dat op hosts niet langer een verzameling wachtwoorden hoeft te worden bijgehouden voor afzonderlijke houders die verificatie vereisen voordat hun toegang kan worden uitgegeven. In plaats daarvan hoeft op de host alleen maar een vertrouwensrelatie te worden ingesteld met een uitgever van certificaten.

Wanneer op een host, zoals een beveiligde webserver, een uitgever wordt aangewezen als vertrouwde basisinstantie, wordt impliciet vertrouwen gesteld in de beleidsregels op basis waarvan de uitgever de

relaties heeft ingesteld in de uitgegeven certificaten. Dit betekent dat erop wordt vertrouwd dat de uitgever de identiteit van de houder van het certificaat heeft gecontroleerd. Wanneer een certificaatuitgever door een host-computer als vertrouwde basisinstantie wordt ingesteld, wordt het zelfondertekende certificaat van de uitgever, dat de openbare sleutel van de uitgever bevat, in het certificaatarchief met vertrouwde basiscertificeringsinstanties van de host geplaatst. Tussenliggende of onderliggende certificeringsinstanties worden alleen vertrouwd als deze een geldig certificaatpad hebben van een vertrouwde basiscertificeringsinstantie.

Entiteit

Een entiteit is een structuur bestaande uit attributen, die een identificeerbare component van een functioneel domein vertegenwoordigen, en staat potentieel in relatie met de andere entiteiten van dit domein.

Een entiteit is een natuurlijke persoon, een rechtspersoon, een systeem of gelijkwaardig.

Hoax

In informatica worden nepberichten of hoax in het Engels meestal verspreid via e-mail of kettingbrief. In dit laatste geval versterkt het internet een fenomeen dat voordien reeds bestond in de klassieke briefwisseling. Het woord hoax is waarschijnlijk een samentrekking van "hocus pocus" en verwijst zo naar bedrog en vervalsing.

Identiteit

Een entiteit kan eenduidig worden geïdentificeerd op basis van één of meerdere identificatieattributen.

Bijvoorbeeld: het rijksregisternummer, het ondernemingsnummer van de Kruispuntbank Ondernemingen (KBO), het erkenningsnummer toegekend door het Rijksinstituut voor Ziekte- en Invaliditeitsverzekering.

Een entiteit bezit slechts één identiteit.

Keystore

Een keystore (sleuteldepot) is een informaticabestand waarin elektronische certificaten worden opgeslagen en eventueel hun private sleutels; de inhoud van dit bestand zal worden gebruikt door toepassingen voor publieke-sleutelvercijfering zoals SSL.

Malware

Malware is de samentrekking van "malicious" (kwaadwillig) en "software". Het gaat om software die ontwikkeld wordt met de bedoeling om schade toe te brengen aan een informaticasysteem. Virussen en wormen zijn de twee meest gekende voorbeelden van malware.

Onweerlegbaarheid

De onweerlegbaarheid betekent dat een actie of gebeurtenis daadwerkelijk plaatsvond en niet nu noch later ontkend kan worden.

Bijvoorbeeld : Het feit van een actie niet te kunnen ontkennen

- de verzender kan niet ontkennen dat hij het bericht heeft verstuurd;
- de ontvanger kan niet ontkennen dat hij het bericht heeft ontvangen;
- de ondertekening van een contract (digitale handtekening).
- ...

Phishing

Phishing is een techniek die gebruikt wordt door fraudeurs om persoonlijke informatie los te krijgen om zich aldus de identiteit van hun slachtoffers toe te eigenen. De techniek bestaat erin het slachtoffer te laten geloven dat het te maken heeft met een betrouwbare instantie - bank, administratie, ... - om op die

manier persoonlijke informatie te achterhalen: paswoord, creditkaartnummer, geboortedatum, enz. Het is een vorm van cyberaanval die berust op social engineering. Phishing kan plaatsvinden via e-mail, via vervalste websites of andere elektronische middelen.

Verantwoordelijke Toegangen Entiteit (VTE)

De Verantwoordelijke Toegangen Entiteit is de persoon die voor de volledige onderneming of organisatie aangesteld is als verantwoordelijke voor alle beveiligde toepassingen die aangeboden worden door de overheid. De Verantwoordelijke Toegangen Entiteit (VTE) is de "root contact" van de onderneming / organisatie. Hij kan één of meerdere hoedanigheden beheren.

SPAM

De term “SPAM” duidt op de massale verspreiding van een bericht voor reclame- of malafide doeleinden, meer bepaald in de vorm van ongewenste e-mail aan de ontvangers. Het niveau van relevantie dat aan een spambericht wordt toegekend varieert van gebruiker tot gebruiker.

Trojan (trojaans paard)

Een Trojan horse is een ogenschijnlijk legitieme software die in werkelijkheid ontwikkeld werd om heimelijk (op een verborgen manier) handelingen uit te voeren zonder dat de gebruiker hiervan weet heeft. Over het algemeen probeert een Trojan horse de rechten van zijn omgeving te gebruiken om gegevens te stelen, te verspreiden of te vernietigen, of om een backdoor te openen aan de hand waarvan een hacker van op afstand de controle over de computer kan overnemen.

Een Trojan horse is geen informaticavirus in die zin dat het zich niet zelf reproduceert, wat wel een essentieel kenmerk is om software als een virus te kunnen beschouwen. Een Trojan horse is ontwikkeld om te worden gereproduceerd wanneer een naïeve gebruiker, die aangetrokken is door de functionaliteiten van het programma, een download of kopie verricht. Een Trojan horse dient heel vaak om een backdoor op een computer te openen. Hierbij wordt dus schade berokkend aan de gebruiker doordat een hacker op elk moment van op afstand (via het internet) de controle over diens computer kan overnemen.Een Trojan horse bestaat uit twee afzonderlijke delen: het servergedeelte en het clientgedeelte. Het clientgedeelte is de component die naar het slachtoffer wordt verstuurd, terwijl het servergedeelte op de computer van de hacker blijft. De client-component wordt via mail verstuurd in de vorm van een software-upgrade (bv. MSN, Adobe Photoshop, Safari, …) of in de vorm van een IQ-test of een winstgevend spel Kortom er bestaan talrijke vormen van. Een Trojan horse sluipt dus de computer binnen en nestelt zich in de registry editor, van waaruit het een backdoor in de computer opent en een verbinding met de computer van de hacker tot stand brengt. Het servergedeelte zorgt voor het versturen van de gegevens. De hacker kan zelf de commando’s bepalen die hij op een pc wenst uit te voeren (hij kan de muis en het toetsenbord controleren, maar ook afprinten, de harde schijf formatteren, een webcam activeren, enz.).

Het onderscheid tussen een Trojan horse, spyware, een keylogger en een backdoor is dus vaak slechts een kwestie van woordgebruik en hangt af van de context.

Worm

In tegenstelling tot een informaticavirus heeft een worm geen “gastprogramma” nodig om zich te reproduceren. Een worm maakt gebruik van de verschillende bestaande of beschikbare middelen om zich te reproduceren. De definitie van een worm slaat enkel op de manier waarop de worm zich van computer naar computer verspreidt.Het eigenlijke doel van dergelijke programma’s kan veel meer zijn dan het zich louter reproduceren. Het doel van een worm kan er namelijk in bestaan te spioneren, een verborgen toegangspunt (backdoor) te openen, gegevens te vernietigen, schade aan te richten, een website te overspoelen met requests zodat de site het begeeft, enz.

Virus

In de strikte zin van het woord is een informaticavirus een informaticaprogramma dat geschreven werd om zich te verspreiden naar andere computers door zich in legitieme gegevens of programma’s te nestelen, de zogenaamde “hosts”. Een informaticavirus kan er ook toe leiden dat er (al dan niet opzettelijk) schade wordt toegebracht doordat het virus de werking van de besmette computer in meer of mindere mate

verstoort. Het virus kan zich verspreiden via elke tool aan de hand waarvan digitale gegevens kunnen worden uitgewisseld, zoals het internet, diskettes, cd-roms, USB-sleutels, enz. Informaticavirussen mogen niet worden verward met wormen. Wormen zijn programma's die zich autonoom kunnen verspreiden en reproduceren zonder daarbij een "gastprogramma" (host program) aan te tasten.

5.2. Bibliografie

1. *Wikipeadia.* [Online] Wikimedia Foundation, Inc. http://nl.wikipedia.org.