Barchman Wuytierslaan 6
3818 LH Amersfoort
www.nedu.nl
T (033) 422 4680

NEDU
Nederlandse Energie Data Uitwisseling

Issue TC033 Softwareveiligheid in de sector

Status	Vastgesteld		
Versienummer	1.0	**Versiedatum**	18 januari 2017
Documentnaam	TC033 Softwareveiligheid in de sector v1.0.docx		

Behandeld door de Technische Commissie

Raakt aan	Kleinverbruik	Grootverbruik	Wholesale
Elektriciteit	**X**	**X**	**X**
Gas	**X**	**X**	**X**

Impact op keten	Ja/Nee
Codewijziging	**Nee**
Berichten	**Nee**
Ketenprocessen	**Nee**

Mogelijke impact marktrollen en EDSN	Ja/Nee
LV	**Ja**
PV	**Ja**
MV	**Ja**
RNB	**Ja**
LNB	**Ja**
EDSN	**Ja**

Vastgesteld door NEDU op	**14 december 2016**
Invoering in markt per	**14 december 2016**

Contact	
Technische Commissie	

Management samenvatting

Het juiste niveau van beveiliging handhaven wordt steeds belangrijker, zeker daar waar gebruik wordt gemaakt van het internet. In de sector kennen we een vrij hoge graad van interactie tussen partijen: informatie wordt uitgewisseld tussen personen onderling, tussen personen en systemen en systemen onderling. Al deze uitwisselingen maken gebruik van internet onder gebruik van diverse protocollen (email, websites, berichtenverkeer, etc.).
De veiligheid en beschikbaarheid van de diverse informatie-uitwisselingen verplicht elke partij in de keten om passende beveiligingsmaatregelen te hanteren. Meer in het bijzonder:

a) Beveiligen van de communicatieketen teneinde een beveiligde en betrouwbare communicatie te waarborgen, waaronder begrepen ook de bescherming van de vertrouwelijkheid via encryptie, de integriteit en authenticiteit via ondertekening door de afzender en de niet-weerlegbaarheid via een ondertekende bevestiging;
b) Afdoende beveiligingsmaatregelen ten uitvoer leggen om onbevoegde toegang tot hun IT-infrastructuur te voorkomen;
c) De andere partijen waarmee zij communiceren onverwijld in kennis stellen van elke onbevoegde toegang die tot hun eigen systeem heeft plaatsgevonden of kan hebben plaatsgevonden.

In de beveiligingswedloop is van belang dat elke partij software gebruikt, welke blootgesteld wordt aan externe netwerken, die voldoet aan de laatste stand van beveiliging, niet alleen voor de eigen beveiliging maar ook voor de beveiliging van de keten. Om die reden heeft de TC een richtlijn voor softwareveiligheid opgesteld.

Situatieschets:

Partijen zijn vrij zelf te bepalen welke softwarepakketten zij gebruiken in de diverse onderdelen in de communicatie in de sector. Echter door de ketenafhankelijkheid kan het voorkomen dat vanwege het feit dat een partij gebruik maakt van een oudere softwareversie of niet gepatchte software ook andere partijen gedwongen worden oudere versies of technologieën te hanteren. Over het algemeen geldt dat oudere versies minder veilig zijn dan recente versies en dat, met name, security patches toegepast moeten worden. Door gebruik te maken van recente, gepatchte, software zullen de beveiligingsrisico's voor de hele sector afnemen.

Vraag:

Kunnen we in de sector afspraken maken zodat ieder de juiste mate van beveiliging kan treffen?

Overwegingen

Er geldt in de sector een hoge graad van ketenafhankelijkheid in de informatie-uitwisseling.
De beveiliging van de ene partij heeft impact op de andere en omgekeerd ook het ontbreken daarvan.
We zijn er als gehele sector samen verantwoordelijk voor om de beveiliging op het juiste niveau te houden: we concurreren immers niet op security!

De meest recente versies en de laatste security patches van een pakket zijn het best bestand tegen de actuele beveiligingsdreigingen.

We realiseren ons dat een partij liever niet de allernieuwste versies (als een van de eersten) installeert, ook omdat er vaak kostbare projecten nodig zijn om vervangingstrajecten te realiseren.

Oplossing:

In het algemeen wordt aangeraden om geen oude software(componenten) te gebruiken, een goede richtlijn is om tenminste actief bijgewerkte software te gebruiken. Omdat versies niet voor elke leverancier dezelfde betekenis hebben en ook (security) patches bijdragen aan de beveiliging zoeken we een methode waarin de kwetsbaarheid (de vulnerability) inzichtelijk is. Partijen kunnen dan aan de hand daarvan besluiten hoe ze het risico mitigeren. Dat kan door software upgrades, patches maar ook door het toevoegen van proxies, firewalls ed. om de software te beschermen tegen misbruik.
Overigens geldt bovenstaande ook voor andere componenten in de keten op het gebied van netwerk, firewalls, operating systemen, etc.

De voorgestelde methode is om de CVE[1] (Common Vulnerabilities and Exposures) databank (http://www.cvedetails.com/) als referentie te gebruiken om in de sector af te spreken dat men maatregelen neemt om de betreffende software/netwerkcomponenten te patchen of te upgraden. Dit is weliswaar een zeer uitgebreide lijst, die zeer frequent wordt aangepast en waaruit men de gebruikte software zelf moet filteren. Een alternatief is gebruik te maken van de adviezen die de NCSC uitgeeft.
Daarnaast geldt in het algemeen om de software(componenten) up to date te houden, nadrukkelijk die software welke (directe of indirecte) invloed heeft op de ketenprocessen en de informatie uitwisseling in de sector, en altijd de laatste security patches toegepast te hebben (binnen een aanvaarde tijdsspanne).

Impact:

Er is geen directe impact op de ketenprocessen.

Invoeringsstrategie:

Elke partij implementeert dit securitybeleid tenminste op software, die (directe of indirecte) invloed heeft op de ketenprocessen en de informatie-uitwisseling in de sector, zo snel mogelijk na vaststelling van het issue.

---

[1] *Common Vulnerabilities and Exposures, meestal afgekort als CVE, is een databank met informatie over kwetsbaarheden in computersystemen en netwerken. Veelal wordt in ook rapporten van penetratietests verwezen naar gegevens in deze databank.*
De databank wordt onderhouden door het bedrijf MITRE Corporation en wordt gefinancierd door de nationale divisie voor informatiebeveiliging van het Amerikaanse Departement van Binnenlandse Veiligheid. CVE wordt gebruikt door het Security Content Automation Protocol, waarmee geautomatiseerd kwetsbaarheden door beveiligingssoftware kunnen worden verwerkt.
Als er nieuwe informatie aan de databank wordt toegevoegd, zal deze eerst gecontroleerd worden. Op de website van CVE wordt dan aangegeven, dat de informatie gereserveerd is, zie https://cve.mitre.org/.

Te vervallen issues:

n.v.t.

Versieoverzicht:

0.1 eerste aanzet door Wim de Olde en Gerrit Fokkema op 6 oktober 2016;
0.2 update na bespreking in de TC van 14 oktober 2016;
0.3 na review door de Security Commissie op 27 oktober 2016;
0.4 verwerking op 25 november 2016 in TC;
1.0 na vaststelling in de ALV van 16 december 2016.