FEDERALE OVERHEIDSDIENST
Werkgelegenheid, Arbeid
en Sociaal Overleg

Arbeidsinspectie
Algemene Directie Toezicht op het welzijn op het werk
Afdeling van het toezicht op de chemische risico's
Ernest Blerotstraat 1 - 1070 Brussel
02 233 45 12 - crc@werk.belgie.be

De impact van cyberaanvallen op de preventie van zware ongevallen

Inhoud

1 Inleiding

Voor de meeste bedrijven is cyberbeveiliging een actueel en gekend thema, aangezien een cyberaanval een belangrijk impact op de activiteit en voortbestaan van het bedrijf kan hebben.

In Seveso-bedrijven is er nog een extra dimensie: een cyberaanval kan immers ook een belangrijke invloed hebben op het vlak van de preventie van zware ongevallen. Cyberdreigingen beïnvloeden de veiligheid van procesinstallaties op diverse manieren:

- door het onbeschikbaar maken van veiligheidsrelevante informatie,
- door het blokkeren van veiligheidsrelevante applicaties,
- of door het verstoren van controle en veiligheidssystemen.

Het streven naar een hoog niveau op het vlak van de preventie van zware ongevallen vraagt dus ook aandacht voor cybersecurity vanuit de invalshoek procesveiligheid.

Deze nota beschrijft een aantal maatregelen om cyberaanvallen met een impact op de preventie van zware ongevallen te voorkomen en om de impact van eventuele geslaagde aanvallen te beperken. De Afdeling van het toezicht op de chemische risico's verwacht dat de Seveso-bedrijven deze maatregelen, voor zover van toepassing, implementeren of alternatieve maatregelen nemen die eenzelfde veiligheidsniveau opleveren.

De term cyberdreiging verwijst naar potentiële risico's en gevaren die voortkomen uit digitale omgevingen. Een cyberdreiging is elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden. Een daadwerkelijke actie die hierop gericht is, wordt een cyberaanval genoemd.

Cyberaanvallen zijn gericht op het stelen, wijzigen of vernietigen van gevoelige informatie of het onderbreken van normale bedrijfsprocessen. Het oogmerk is in de meeste gevallen het afpersen van het slachtoffer voor geld, maar aanvallen die er enkel op gericht zijn schade te berokkenen zijn ook mogelijk.

Er zijn verschillende soorten cyberaanvallen en aanvalsroutes. Voor de meeste cyberaanvallen is het noodzakelijk dat de aanvaller toegang verwerft tot het aan te vallen systeem. Toegang tot systemen kan gebeuren vanop afstand via het internet of door zich fysiek toegang te verschaffen tot het netwerk.

De meeste cybersecuritymaatregelen zijn dus gericht op het voorkomen van ongewenste (digitale en/of fysieke) toegang. Belangrijk is het te voorkomen dat software die toegangsmaatregelen kan omzeilen via een andere weg binnengeraakt. (USB-sticks, besmette software of software-updates, …).

Er bestaan ook zogenaamde "Denial of Service" aanvallen, waarbij de netwerkinfrastructuur zoals servers of routers bestookt worden met een dusdanig grote stroom aan gegevens, dat ze overbelast geraken en hun normale functie niet meer kunnen uitoefenen.

Een lijst van concrete tegenmaatregelen om de risico's van cyberaanvallen te verminderen, kan men aantreffen in het Cyberfundamentals Framework dat gepubliceerd wordt door het Center for Cybersecurity Belgium (CCB)[1]. Dit framework helpt organisaties om te voldoen aan de vereisten van de NIS 2 wetgeving[2].

[1] https://ccb.belgium.be/

[2] De wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid

2 Veiligheidsrelevante informatie

Veiligheidsrelevante informatie is informatie die noodzakelijk is voor het functioneren van het veiligheidsbeheersysteem (en de preventie van zware ongevallen in de breedste zin).

Enkele voorbeelden van veiligheidsrelevante informatie zijn:

- de procedures en instructies die het veiligheidsbeheerssysteem beschrijven
- instructies voor het uitbaten, inspecteren en onderhouden van de installaties
- risicoanalyses
- inspectie- en onderhoudsprogramma's
- het noodplan
- technische specificaties van alle onderdelen van de installatie (omhullingen, controlesystemen, instrumentele en mechanische veiligheidssystemen)
- P&ID's, isometrieën en andere constructietekeningen
- informatie over gevaren van gevaarlijke stoffen en de reacties
- registraties van inspecties, onderhoudsbeurten, herstellingen
- registraties van opleidingen
- registraties van noodplanoefeningen
- resultaten van interne en externe audits

2.1 De impact van cyberaanvallen

Een cyberaanval die (een deel van) de veiligheidsrelevante informatie onbeschikbaar maakt, zal niet rechtstreeks aanleiding geven tot een zwaar ongeval. Indien deze informatie echter gedurende langere tijd onbeschikbaar blijft, kan de impact echter wel belangrijk worden. Het onbeschikbaar zijn van veiligheidsrelevante informatie kan een onderliggende oorzaak zijn van een procesincident en mogelijk van een zwaar ongeval.

Het verlies van veiligheidsrelevante informatie heeft een dubbele impact: niet alleen brengt het de goede werking van het veiligheidsbeheersysteem in gevaar, het zorgt er ook voor dat het bedrijf niet kan aantonen aan bevoegde overheden, waaronder de inspectiediensten, dat de nodige maatregelen vereist door het Seveso-samenwerkingsakkoord werden genomen.

Met het oog op de beheersing van cyberincidenten is het belangrijk om na te gaan in welke mate deze informatie al dan niet tijdelijk kan gemist worden. Men kan hierbij de volgende indeling maken:

- informatie die permanent beschikbaar moet zijn,
- informatie die noodzakelijk is om bepaalde activiteiten uit te voeren (productie en ondersteunende activiteiten) en
- informatie die gedurende een zekere tijd gemist kan worden alvorens het ontbreken ervan noopt tot het stopzetten van bepaalde activiteiten.

Informatie die noodzakelijk is om de installatie op een veilige wijze tot stilstand te brengen en informatie over de restrisico's van de stilgelegde installaties (waarin nog gevaarlijke producten aanwezig zijn) zou permanent beschikbaar moeten zijn. Denk hierbij aan de volgende informatie:

- instructies om een installatie tot stilstand te brengen
- noodplan met inbegrip van de interventiescenario's en bijhorende instructies
- situatieplannen met de aanwezigheid van gevaarlijk stoffen
- informatie over de gevaren van stoffen en reacties
- P&ID's
- plannen van de riolering, bluswaternetten, gasdetectiesystemen

De lijst is niet exhaustief. Elke onderneming moet zelf een analyse maken van de documenten die steeds beschikbaar zouden moeten zijn.

2.2 Preventie van cyberincidenten

Deze informatie – voor zover ze bewaard wordt op digitale dragers – bevindt zich typisch in het IT-netwerk van het bedrijf. Ze is dus kwetsbaar voor cyberaanvallen en de beveiliging hangt af van de beveiliging van het IT-netwerk.

Het beschrijven van de aanpak die noodzakelijk is om IT-netwerken te beschermen, valt buiten het bestek van deze nota. Enkele aspecten die hierin steeds aan bod komen zijn o.a.:

- identiteits- en toegangsbeheer
- opleiding
- monitoring
- updatestrategie

Een lijst van concrete tegenmaatregelen om de risico's van cyberaanvallen te verminderen, kan men aantreffen in het Cyberfundamentals Framework dat gepubliceerd wordt door het Center for Cybersecurity Belgium.

2.3 Incidentbeheersing

Ondanks de inspanningen die men treft om cyberaanvallen te voorkomen, dient men rekening te houden met de mogelijkheid van geslaagde cyberaanvallen en dus met de mogelijkheid dat bepaalde informatie hierdoor niet meer beschikbaar is in digitale vorm.

2.3.1 Papieren back-ups

De beschikbaarheid van informatie die permanent aanwezig moet zijn (ook in geval van een geslaagde cyberaanval) kan verzekerd worden door deze informatie (ook) in papieren vorm bij te houden en ter beschikking te stellen.

Daarbij is het nodig dat de gebruikers op de hoogte zijn van de papieren exemplaren, ze deze gemakkelijk kunnen vinden en raadplegen. Uiteraard moet het nodige gedaan worden om te zorgen dat deze informatie steeds actueel is.

2.3.2 Stopzetten of niet uitvoeren van bepaalde activiteiten

Als men heeft geoordeeld dat bepaalde informatie noodzakelijk is om bepaalde activiteiten uit te voeren, dan volgt daaruit dat deze activiteiten moeten stopgezet worden als die noodzakelijke informatie niet beschikbaar is.

Analoog kunnen nieuwe activiteiten niet worden opgestart zolang de daartoe noodzakelijke informatie niet beschikbaar is.

2.3.3 Digitale back-ups

Het permanente verlies van digitale veiligheidsrelevante informatie kan voorkomen worden door de nodige back-ups te voorzien.

Het herinstalleren van back-ups na een cyberaanval is een proces dat met de nodige voorzichtigheid moet gebeuren. Er dient nagegaan te worden of de back-up zelf ook niet geïnfecteerd is met malware. Als er na een geslaagde aanval vele systemen en informatiedragers getroffen zijn, kan het dus een zekere tijd duren voor dat alle back-ups zijn vrijgegeven. Bij het bepalen van de volgorde voor het controleren en vrijgeven van back-ups zou men ook rekening moeten houden met de veiligheidsconsequentie van het niet ter beschikking hebben van bepaalde informatie. Sommige veiligheidsrelevante informatie zal men sneller terug beschikking willen hebben. Het bepalen van de prioriteit voor het vrijgeven van back-ups zou deel moeten uitmaken van het cybersecuritybeleid van de onderneming.

3 Veiligheidsrelevante informaticatoepassingen

Veiligheidsrelevante informaticatoepassingen zijn toepassingen die een rol spelen in het veiligheidsbeheersysteem ter preventie van zware ongevallen.

Voorbeelden zijn:

- Het elektronisch werkvergunningssysteem
- Systemen voor toegangscontrole en -aanwezigheidsregistratie
- Planningssystemen (onderhoud, inspectie, opleiding, personeelsbezetting, …)
- Systemen voor stockbeheer en productieplanning
- Systemen voor projectmanagement (beheer van wijzigingen)

3.1 De impact van cyberaanvallen

Een cyberaanval die één of meer veiligheidsrelevante toepassingen buiten werking stelt, zal, net als in het geval van veiligheidsrelevante informatie, niet rechtstreeks aanleiding geven tot een zwaar ongeval. Indien deze toepassingen echter gedurende langere tijd onbeschikbaar blijven, kan de impact echter wel belangrijk worden. Het onbeschikbaar zijn van veiligheidsrelevante informaticatoepassingen kan een onderliggende oorzaak zijn van een procesincident en mogelijk van een zwaar ongeval.

Er moet mee rekening gehouden worden dat een cyberaanval meerdere systemen gelijktijdig kan treffen en dat het enige tijd kan duren alvorens de getroffen systemen terug operationeel kunnen gemaakt worden.

In dit opzicht is het belangrijk een analyse te maken van het kritieke karakter van de informaticatoepassingen:

- welke toepassingen bieden functionaliteiten die permanent beschikbaar moeten zijn om de installaties (of bepaalde delen ervan) in werking te laten,
- welke toepassingen bieden functionaliteiten die noodzakelijk zijn om bepaalde ondersteunende activiteiten toe te laten en
- welke toepassingen kunnen gedurende een bepaalde tijd gemist worden alvorens het ontbreken ervan noopt tot het stopzetten van bepaalde activiteiten.

3.2 Preventie van cyberincidenten

Veiligheidsrelevante informaticatoepassingen bevinden zich typisch in het IT-netwerk van het bedrijf. Ze zijn dus kwetsbaar voor cyberaanvallen en de beveiliging hangt af van de beveiliging van het IT-netwerk.

Het beschrijven van de aanpak die noodzakelijk is om IT-netwerken te beschermen, valt buiten het bestek van deze nota. Een lijst van concrete tegenmaatregelen om de risico's van cyberaanvallen te verminderen, kan men aantreffen in het Cyberfundamentals Framework dat gepubliceerd wordt door het Center for Cybersecurity Belgium.

3.3 Incidentbeheersing

Ondanks de inspanningen die men treft om cyberaanvallen te voorkomen, dient men rekening te houden met de mogelijkheid van geslaagde cyberaanvallen en dus met de mogelijkheid dat bepaalde informaticatoepassingen hierdoor niet meer beschikbaar zijn.

Voor toepassingen die noodzakelijk zijn voor het uitvoeren van bepaalde activiteiten, zijn er 2 opties:

- Het voorzien in een alternatieve werkwijze, die niet afhankelijk is van een informaticatoepassing; bijvoorbeeld een papieren werkvergunningssysteem als back-up voor een elektronisch werkvergunningssysteem of een aanwezigheidsregistratie op papier.
- Het tijdelijk stopzetten van de activiteit zolang de toepassing niet operationeel is.

De keuze is afhankelijk van het kritieke karakter van de activiteit. Sommige activiteiten kunnen niet gedurende lange tijd worden stopgezet zonder impact op de preventie van zware ongevallen (opleiding, onderhoud, inspectie, …).

4 Controle- en veiligheidssystemen

In procesinstallaties spreken we over instrumentele controle- en veiligheidssystemen. Deze worden geïmplementeerd via allerlei diverse programmeerbare digitale systemen, waaronder Distributed Control Systems (DCS), Programmable Logic Solvers (PLC) of Supervisory Control and Data Acquisition systems (SCADA).

Het is courante praktijk dat instrumentele controlesystemen verbonden zijn met interne bedrijfsnetwerken, die op hun beurt verbonden zijn met externe netwerken. Op die manier worden controlesystemen vatbaar voor cyberaanvallen.

Instrumentele veiligheidssystemen hebben als doel om in te grijpen als er door het falen van het controlesysteem een gevaarlijke afwijking optreedt van de normale werking van de installatie. Instrumentele veiligheidssystemen dienen daarom onafhankelijk worden uitgevoerd van controlesystemen. De onafhankelijkheid van veiligheidssystemen moet voorkomen dat eenzelfde fout beide systemen tegelijkertijd uitschakelt, en dus aanleiding zou geven tot een gevaarlijke afwijking die niet gecorrigeerd wordt door het veiligheidssysteem.

De instrumentele controle- en veiligheidssystemen maken deel uit van wat “Operationele Technologie” of “OT”-systemen genoemd wordt. Daaronder verstaan we de hardware en software die gebruikt worden om industriële apparatuur en systemen te beheren, bijvoorbeeld voor het aansturen van pompen, het uitlezen van sensoren, het schakelen van kleppen enz. In de literatuur wordt ook gesproken over “Industrial Automation and Control Systems” (IACS).

4.1 De impact van cyberaanvallen

Door de verschillen in technologie, vraagt een cyberaanval die een OT-systeem wil compromitteren meer kennis van de aanvaller. Dit zorgt ervoor dat er minder aanvallen worden uitgevoerd die gericht zijn op deze systemen. Het is echter wel mogelijk. In 2017 werd een petrochemische fabriek in Saudi-Arabië het slachtoffer van een cyberaanval met een zogenaamde “malware” genaamd Triton[3]. Deze malware was uitdrukkelijk gericht op de instrumentele beveiligingen van de installaties. Door een fout in de code was het gevolg van de aanval alleen maar een automatische stop van de installaties, maar het is duidelijk dat de gevolgen veel ernstiger hadden kunnen zijn. Andere gekende voorbeelden van aanvallen op industriële installaties zijn Stuxnet[4] en Havex[5].

4.1.1 Impact op controlesystemen

Een cyberaanval op het controlesysteem van een procesinstallatie kan ertoe leiden dat het systeem verkeerd functioneert of in zijn geheel stopt met functioneren. Het gevolg is het optreden van één of meerdere processtoringen. Een processtoring zou op zich niet direct mogen leiden tot een incident of ongeval, op voorwaarde dat de nodige veiligheden werden voorzien en dat deze functioneren op het moment dat ze worden aangesproken.

Belangrijk hierbij is dat cyberaanvallen meerdere systemen gelijktijdig kunnen compromitteren. Dit zorgt ervoor dat ze aanleiding kunnen geven tot het gelijktijdig optreden van meerdere schijnbaar niet gerelateerde afwijkingen, wat in een klassieke procesveiligheidsstudie als onwaarschijnlijk zou beschouwd worden.

[3] https://en.wikipedia.org/wiki/Triton_(malware)
[4] https://en.wikipedia.org/wiki/Stuxnet
[5] https://en.wikipedia.org/wiki/Havex

De betrouwbaarheid van actieve veiligheidssystemen is eindig, en bij elke processtoring bestaat een (in principe kleine) kans dat ze leidt tot een incident of ongeval. Vanuit dat standpunt is het voorkomen van cyberaanvallen op de controlesystemen niet alleen vanuit operationeel standpunt maar ook vanuit veiligheidstandpunt belangrijk.

De analyse van dit risico kan deel uitmaken van de procesrisicoanalyse (vb. HAZOP) of gebeuren in een aparte cybersecurity-analyse.

4.1.2 Impact op veiligheidssysteem

Een cyberaanval op een veiligheidssysteem kan ertoe leiden dat het systeem wordt uitgeschakeld of dat er een fout wordt geïntroduceerd in de werking ervan. Een aanval op een veiligheidssysteem leidt in principe niet onmiddellijk tot een procesincident. Het is pas wanneer het uitgeschakelde of fout werkende veiligheidssysteem wordt aangesproken (door het optreden van een storing in het controlesysteem) dat er zich een probleem voordoet. Bijzonder gevaarlijk in dat opzicht zijn de niet-gedetecteerde ("slapende") fouten in het veiligheidssysteem. Als een cyberaanval op het veiligheidssysteem wordt gedetecteerd, dient men onmiddellijk de veiligheidssystemen te onderzoeken en te testen op fouten.

Een cyberaanval die tegelijkertijd het controlesysteem als het veiligheidssysteem zou aantasten, leidt tot een zeer gevaarlijke situatie, waarbij processtoringen kunnen optreden waarop niet (correct) gereageerd wordt door het veiligheidssysteem.

4.2 Preventie van cyberincidenten

Hieronder beschrijven we enkele typische maatregelen die getroffen worden om te vermijden dat cyberaanvallen in procesinstallaties zouden kunnen leiden tot een zwaar ongeval. Deze oplijsting is zeker niet exhaustief.

Net als de veiligheidsfuncties in procesveiligheid (zoals beschreven in de informatienota CRC/IN/002 "Procesveiligheidsstudie"[6]), vraagt de aanpak van cyberveiligheid in een procesinstallatie om de toepassing van meerdere beschermingslagen ("defense in depth").

De belangrijkste aspecten die hier aan bod komen zijn isolatie van systemen, toegangscontrole en softwaremanagement.

Bij de maatregelen die we hier beschrijven, gaan we uit van cyberaanvallen met een "willekeurig" of "ongericht" karakter. Daarmee bedoelen we: aanvallen die niet specifiek zijn opgezet met het doel om zware ongevallen te veroorzaken. Cyberaanvallen die uitgevoerd worden met als doel om scenario's van zware ongevallen (m.a.w. chemische rampen) uit te lokken, eventueel in combinatie met bepaalde fysieke sabotageacties uitgevoerd in de installaties en met hulp van binnen het bedrijf, zijn een vorm van terrorisme.

Het voorkomen van terroristische aanvallen valt volgens de Afdeling van het toezicht op de chemische risico's niet onder het toepassingsgebied van de Seveso-richtlijn en haar omzetting in Belgisch recht (het "Seveso-samenwerkingsakkoord"). De Seveso-richtlijn gaat immers over de preventie van (zware) ongevallen, en de meeste definities van ongevallen vermelden het niet-intentionele karakter van dergelijke gebeurtenissen. Of de terroristische aanval wordt uitgevoerd door een fysieke sabotagedaad of aanval, een virtuele aanval of een combinatie van beiden maakt voor die interpretatie geen verschil.

4.2.1 Netwerksegmentatie

Een aantal recente evoluties (toegang vanop afstand, data analytics, kunstmatige intelligentie (AI), …) zorgen er voor dat OT- en IT-netwerken meer en meer geïntegreerd geraken. Deze convergentie vergroot het digitale aanvalsoppervlak. Aanvallen gericht op IT-netwerken hebben het potentieel om ook OT-systemen te raken.

[6] https://werk.belgie.be/nl/publicaties/informatienota-procesveiligheidsstudie

Het is een goede praktijk om het OT-netwerk te scheiden van het bedrijfsnetwerk via een zogenaamde DMZ ("Demilitarized Zone"). De DMZ controleert enerzijds het verkeer tussen het bedrijfsnetwerk en de DMZ en anderzijds het verkeer tussen de DMZ en het OT-netwerk. Door deze dubbele barrière wordt ervoor gezorgd dat zelfs als een aanval één barrière passeert, het OT-netwerk niet onmiddellijk gecompromitteerd is. Uiteraard veronderstelt dit dat de nodige monitoring aanwezig is zodat de eerste doorbraak gedetecteerd wordt vooraleer een aanvaller ook de tweede barrière kan verslaan.

Een verder doorgedreven segmentatie, zoals een fysieke afscheiding en/of elektronische onderbreking tussen het netwerk met controlesystemen en het netwerk met veiligheidssystemen kan in functie van de aard en de risico's van de procesinstallaties aangewezen zijn.

4.2.2 Toegangscontrole

Analoog als de dubbele barrière in bovenstaande netwerksegmentatie is het ook belangrijk ervoor te zorgen dat indien een aanvaller erin zou slagen om toegangsgegevens te bemachtigen van een gebruiker op het IT-netwerk, hij hiermee niet onmiddellijk ook toegang verkrijgt tot het OT-netwerk. Om dit te realiseren is het belangrijk dat de verschillende netwerken gebruiken maken van aparte accounts en aparte sterke wachtwoorden.

Een belangrijk aandachtspunt hierbij is de opleiding van alle betrokken gebruikers, zowel bij het eigen personeel als bij toeleveranciers. De mens is nog steeds de meest voorkomende toegangsweg voor cyberaanvallen. Phishingmails zijn een veel gebruikte techniek om toegangsgegevens te bemachtigen. Het is dan ook belangrijk gebruikers hierover op te leiden en waakzaam te houden.

4.2.3 Onafhankelijkheid van veiligheidssystemen

Hierboven werd reeds gewezen op het belang van de onafhankelijkheid tussen controle- en veiligheidssystemen. Dat is een fundamenteel principe van de veiligheidswetenschap in het algemeen en van procesveiligheid in het bijzonder. Die onafhankelijkheid blijkt nu ook van cruciaal belang voor de bescherming tegen cyberaanvallen.

De grootste mate van onafhankelijkheid wordt gegarandeerd door volgende maatregelen:

- Aparte hardware voor instrumentele veiligheidssystemen, gescheiden van de hardware voor controlesystemen
- De communicatie tussen het controlesysteem en het veiligheidssysteem laat niet toe om wijzigingen aan te brengen aan het veiligheidssysteem
- Beperkte toegang tot de veiligheidssystemen (enkel voor gespecialiseerd en bevoegd personeel).
- Strikte procedures voor het aanbrengen van wijzigingen aan instrumentele veiligheidssystemen, waarbij wijzigingen formeel worden gevalideerd alvorens ze worden geïmplementeerd en waarbij na implementatie de goede werking wordt getest.

De onafhankelijke uitvoering van de veiligheidssystemen zoals hierboven beschreven laat ook toe om deze systemen los te koppelen van interne of externe netwerken, en daarmee de belangrijkste aanvalsroute voor cyberaanvallen af te sluiten. De programmering gebeurt dan ter plaatse via werkstations die enkel voor dat doeleinde gebruikt worden en die ontdaan zijn van alle software die hiervoor niet nodig is. Het risico op besmetting van deze werkstations wordt hierdoor zeer sterk teruggedrongen.

Mechanische beveiligingen (zoals veiligheidskleppen) zijn niet kwetsbaar voor digitale aanvallen. Het toepassen van diversiteit in de keuze van de beveiligingslagen in procesinstallaties, waarbij de "last line of defense" van mechanische aard is, is een courante goede praktijk.

4.2.4 Software management

Een kritisch aspect van de cybersecurity in OT-systemen is het software beheer. Dit omvat enerzijds het verwijderen van onnodige services en programma's en anderzijds het updaten van software om kwetsbaarheden weg te werken. Dit laatste wordt ook wel "patch management" genoemd, en omvat het

proces van identificeren, prioriteren, testen, implementeren en verifiëren van softwarepatches. De belangrijkste reden voor het implementeren van patchbeheer is ervoor te zorgen dat kwetsbaarheden in software tijdig en effectief worden verholpen. Patches worden meestal uitgebracht door softwareleveranciers als reactie op nieuw ontdekte kwetsbaarheden of bugs. Deze kwetsbaarheden kunnen door aanvallers worden misbruikt om ongeautoriseerde toegang tot systemen te krijgen, gegevens te stelen of schade te veroorzaken. Daarom is het tijdig patchen van kwetsbaarheden cruciaal voor het behoud van de veiligheid en integriteit van digitale systemen.

De levenscyclus van OT-systemen is heel verschillend van deze van IT-systemen. OT-systemen hebben over het algemeen een veel langere levensduur (typisch 20 jaar tegenover 5 jaar in IT). Dit betekent dat in vele gevallen de gebruikte technologie minder modern is dan in IT-systemen, dat er meer variatie is in de aanwezige OT-systemen en dat systemen soms geen leveranciersondersteuning meer hebben.

Doordat OT-systemen verbonden zijn aan procesinstallaties, is het updaten van hardware en software van deze systemen gebonden aan o.a. de productiestilstanden van deze installaties. Gezien de complexiteit van OT-systemen, zorgt het patchen vaak voor een aanzienlijke downtime. Patches moeten zorgvuldig gepland worden om de productieprocessen niet te verstoren. Zeker voor continue procesinstallaties heeft dit voor gevolg dat bijvoorbeeld het toepassen van updates gericht op het corrigeren van gekende kwetsbaarheden veelal niet onmiddellijk mogelijk is. Vastgestelde kwetsbaarheden in software moeten eventueel tijdelijk worden opgevangen via andere maatregelen.

Er is ook een zeker risico: een onjuiste patch kan leiden tot systeemstoringen en eventueel gevaarlijke situaties. Daarom moeten patches vooraf grondig worden getest.

De familie van internationale standaarden IEC62443 beschrijft een reeks technische en organisatorische aspecten eigen aan de aanpak van cybersecurity in automatisatie en controlesystemen. De IEC 62443-2-3 norm geeft richtlijnen voor het ontwikkelen van een patchmanagementprogramma.

4.3 Incidentbeheersing

De incidentbeheersing bij een cyberaanval waarbij het OT-systeem gecompromitteerd wordt, moet er uiteraard in de eerste plaats op gericht zijn te voorkomen dat de aanval zou leiden tot een belangrijk procesincident. Dit betekent dat nodige acties moeten kunnen getroffen worden om de installaties alsnog op een veilige manier tot stilstand te brengen. In de noodprocedures die hiervoor ontwikkeld worden, moet worden rekening gehouden dat één of meerdere controle- of veiligheidssystemen onbeschikbaar kunnen zijn of zelfs foutief kunnen reageren.

Een eerste voorwaarde is hierbij uiteraard dat verdachte activiteiten tijdig worden gedetecteerd. Dit kan o.a. via de implementatie van een intrusiedetectiesysteem (IDS).

Verder verhoogt de aanwezigheid van cyberrisico's het belang om bij het ontwerp van procesinstallaties het failsafe-principe te respecteren.

Een fysieke noodstop kan in vele gevallen een belangrijke rol spelen bij het stoppen van het proces in geval van een ernstige cyberaanval. Deze noodstop kan handmatig worden geactiveerd en werkt onafhankelijk van het controlesysteem.

Indien installaties worden stilgelegd ten gevolge van een cyberaanval, is het noodzakelijk dat het herstelplan een doorgedreven evaluatie van alle controle- en veiligheidssystemen omvat. Een functionele test van alle beveiligingen is nodig vooraleer installaties terug worden opgestart.

Deze nota verschijnt in de reeks “Informatienota’s” van de Afdeling van het toezicht op de chemische risico’s.

Deze informatienota's worden opgesteld om verduidelijkingen te geven over bestaande reglementering, om toelichting te geven omtrent nieuwe regelgeving, om de bedrijven attent te maken op bepaalde aspecten van de preventie van zware ongevallen of om de visie van de Afdeling van het toezicht op de chemische risico's over een bepaalde problematiek weer te geven. Deze informatienota's dienen eerder als verheldering gezien te worden en hebben geen verplichtend karakter.

Meer informatie over de preventie van zware ongevallen vindt u op: www.werk.belgie.be/nl/acr

Deze nota mag vrij verspreid worden op voorwaarde dat het om de volledige nota gaat.

Cette note est aussi disponible en français.

De redactie werd afgesloten op 20 december 2024.

Kenmerk: CRC/IN/021-N – versie 1

Verantwoordelijke uitgever: FOD Werkgelegenheid, Arbeid en Sociaal Overleg

Wettelijk depotnr: D/2024/1205/08