EIWTC · CER / NIS-2 / CRA

Transkript vum Podcast

Cyber- und Sabotageschutz im Wasserwerk

Lëtzebuergesch – Iwwersetzung vun der iwwerschaffter Versioun

Iwwersetzung vun der iwwerschaffter däitscher Textfassung op Basis vun der agereechter PDF; net Wuert fir Wuert mat der Tounopnam verglach. Fachinformatiounen, keng Rechtsberodung.

Inhaltsiwwersiicht

01 · Begréissung, den Hannergrond an de Kader
02 · D’Unname vum Modell an d’All-Hazards-Approche
03 · National Strategie: Zesummespill vu CER, NIS-2 a CRA
04 · D’Gesetzer vum 5. Mee 2026, d’Artikelen an d’Verantwortung
05 · De Prinzip vun de Schutzschichten an de Liewenszyklus vun den Zougangsrechter
06 · Grenze vun der Mechanik, Stand vun der Technik a Reifegraden
07 · Systemopbau, Kryptografie an d’Roll vum CRA
08 · Déi dräi praktesch Auditfäll am Detail
09 · Meldeflichten a zoustänneg Stellen: 24 Stonnen, 72 Stonnen, ee Mount
10 · Den Ëmsetzungsplang iwwer 90 Deeg a véier Decisioune fir d’Leedung
11 · Vertiefungen: DORA, speziell Reegele an technesch Themen

Kapitel 1: Begréissung, den Hannergrond an de Kader

Moderator (Chris)
Häerzlech wëllkomm bei eiser Spezialeditioun vum Podcast iwwer kritesch Infrastrukturen a Resilienz! Haut schwätze mir iwwer e Sujet, deen op den éischte Bléck ganz praktesch an alldeeglech wierkt. Wann ee méi genee hikuckt, verbënnt en awer d'digital Cybersécherheet, de physesche Schutz géint Sabotage an déi staatlech Reguléierung: d'Zougangskontroll a kriteschen Infrastrukturen, erkläert um konkrete Beispill vun engem Waasserwierk.

Klaus Wollscheid
Moien Chris, villmools Merci fir d'Invitatioun! Et freet mech, haut hei ze sinn. Als CEO vun EIWTC SARL an CSO vu BEWENG S.A. beschäftegen ech mech all Dag genee mat dëser Schnëttstell. Egal ob am Waasserwierk, am Spidol oder am Rechenzentrum: Eng Dier, déi ouni Berechtegung opgemaach gëtt, kann am schlëmmste Fall eng ganz wichteg Versuergung zum Stëllstand bréngen.

Moderator (Chris)
Klaus, mir hunn haut e wierklech ëmfangräiche Programm virun eis. Zanter de neie Lëtzebuerger Gesetzer vum 5. Mee 2026, mat deenen déi europäesch CER- an NIS-2-Richtlinnen an nationaalt Recht ëmgesat goufen, an dem EU-Cyber-Resilience-Act, kuerz CRA, stinn d'Bedreiwer viru ganz konkrete rechtlechen an technesche Flichten. Mir wëllen all Detail ukucken: vum Prinzip vun de Schutzschichten iwwer de Liewenszyklus vun den Zougangsrechter bis bei praktesch Auditfäll an d'Sonderreegelen aus de Reservefolien.

Klaus Wollscheid
Absolut! A virun allem bleiwe mir net bei der Theorie. Mir erklären dat un engem ganz anschauliche Modell: eisem fiktiven, awer realistesche kritesche Waasserwierk. Do geet et ëm näischt manner wéi d'Oprechterhale vun enger onënnerbrachener Drénkwaasserversuergung fir d'Bevëlkerung.

Kapitel 2: D’Unname vum Modell an d’All-Hazards-Approche

Moderator (Chris)
Da fänke mir direkt beim Waasserwierk un. Wéi eng Plazen a Beräicher gehéieren zu eisem Beispill?

Klaus Wollscheid
Fir eise Modell gi mir dovun aus, datt d'Waasserwierk offiziell als kritesch Ariichtung benannt gouf. D'Anlag huet typescherweis véier Haaptberäicher. Éischtens d'Paart vum Terrain, wou Visiteuren empfaangen a begleet ginn. Zweetens d'Betribsgebai, wou Techniker Zougangsrechter fir hire konkreten Optrag kréien. Drëttens d'zentral Leitstell, wou d'Betribspersonal d'Versuergung ronderëm d'Auer oprechterhält a wou den Ënnerhalt just no enger formeller Fräigab stattfënnt. A véiertens d'Häerzstéck: déi eigentlech Steierung an d'Sensorik. Zousätzlech huele mir nach eng ofgeleeë Pompelstatioun un, där hir Netzwierkverbindung zäitweis ënnerbrach ass.

Moderator (Chris)
Dat kléngt ganz no un der Praxis! Firwat ass d'Zougangskontroll an esou engem Opbau esou entscheedend? Wat kann do schifgoen?

Klaus Wollscheid
Am moderne Sécherheetsmanagement schwätze mir vun der All-Hazards-Approche. Dobäi gi physesch an digital Risiken zesumme gekuckt. Kucke mir eis eng méiglech Kette un: Eng verluer oder geklaute Mataarbechterkaart bleift am System valabel. Eng Persoun ouni Berechtegung benotzt se, fir duerch eng Dier ze kommen. Si erreecht e Steierungsschaf oder en oppenen Netzwierkuschloss am Betribsgebai. Do manipuléiert si eng Anlag oder bréngt schiedlech Software eran. D'Resultat ass e plëtzlechen Ausfall vun der Steierung an eng Stéierung vun der Drénkwaasserversuergung! Eng net genuch geséchert Dier kann esou direkt zu engem IT-Ausfall an zum Ënnerbroch vun der Versuergung féieren.

Moderator (Chris)
D'All-Hazards-Approche geet awer nach vill méi wäit wéi klassesch Sabotage, oder?

Klaus Wollscheid
Genee. Nieft Cyberattacken a geziilter Sabotage bewäerte mir och Naturgefore wéi Héichwaasser, Stroumausfäll, Personalausfäll duerch Pandemien a Liwwerengpäss. Alles muss am Zesummenhang bewäert ginn: d'Méiglechkeete fir eranzekommen, d'Ofhängegkeeten, d'Folgen an déi konkret Pläng fir den Neistart.

Kapitel 3: National Strategie: Zesummespill vu CER, NIS-2 a CRA

Moderator (Chris)
Domat si mir direkt beim rechtlechen a strategesche Kader. Lëtzebuerg huet eng national Resilienzstrategie mat aacht Sailen ugeholl. Wéi passen eis Gesetzer do eran?

Klaus Wollscheid
Lëtzebuerg deelt seng Resilienz an aacht Sailen an: Sail 1, Demokratie, Rechtsstaat a Regierung; Sail 2, eng resilient Gesellschaft; Sail 3, d'Sail fir CER, also wesentlech Déngschter a kritesch Infrastrukturen; Sail 4, eng resilient Wirtschaft; Sail 5, strategesch a logistesch Ressourcen; Sail 6, d'Sail fir NIS-2 an d'Cyberresilienz; Sail 7, zivil Verdeedegung; a Sail 8, Schutz a Verdeedegung vum eegenen Territoire. Den Ënnerscheed ass kloer: CER schützt déi physesch a betriblech Versuergung, NIS-2 schützt déi digital Netzer a Systemer, an de Cyber Resilience Act, CRA, stäerkt d'Sécherheet vun den agesaten digitale Produkter.

Moderator (Chris)
Wéi eng Secteure falen zu Lëtzebuerg ënner dës Reegele?

Klaus Wollscheid
CER ëmfaasst zwielef Secteuren: Energie, Transport, Bankewiesen, Finanzmaartinfrastrukturen, Gesondheet, Drénkwaasser, Ofwaasser, digital Infrastrukturen, ëffentlech Verwaltung, Weltraum, Liewensmëttel an Offallbewirtschaftung. NIS-2 ëmfaasst vill vun dëse Beräicher a weider Secteuren, dorënner: IKT-Déngschter fir Entreprisen, Post- a Courrierdéngschter, Chemikalien, bestëmmte Produktiounsberäicher, digital Ubidder a Fuerschung. Dat ass eng vereinfacht Iwwersiicht vun de Secteuren. Ob eng konkret Ariichtung ënner d’Reegelen fält, hänkt vun der Aart vun der Ariichtung, de Gréisstkritären an de gesetzleche Spezialreegelen of.

Moderator (Chris)
Wéi ginn d'Ariichtungen an dëse Secteuren agestuuft? Et ginn d'Begréffer „kritesch“, „wesentlech“ a „wichteg“.

Klaus Wollscheid
Dat ass e ganz entscheedende Punkt fir d'Auditen! Bei CER schwätze mir vun enger „kritescher Ariichtung“. Si gëtt vum Staat formell benannt, jee no hirer Bedeitung fir d'Gesellschaft. NIS-2 ënnerscheet tëscht „wesentlechen Ariichtungen“ – normalerweis grouss Entreprisen aus dem Annexe I oder Ariichtunge mat engem spezielle gesetzleche Statut – an „wichtegen Ariichtungen“, beispillsweis mëttelgrouss Entreprisen aus dem Annexe I a mëttelgrouss oder grouss Entreprisen aus dem Annexe II. Fir eist Waasserwierk gëllt e wichtege Grondsaz: Soubal et ënner CER offiziell als kritesch benannt ass, gëllt et ënner NIS-2 automatesch als „wesentlech Ariichtung“, onofhängeg vun der Zuel vu Mataarbechter oder vum Ëmsaz!

Kapitel 4: D’Gesetzer vum 5. Mee 2026, d’Artikelen an d’Verantwortung

Moderator (Chris)
Komme mir bei déi konkret rechtlech Grondlagen zu Lëtzebuerg. Wéi en Datum solle Sécherheetsverantwortlech sech rout am Kalenner umaachen?

Klaus Wollscheid
De 5. Mee 2026! Deen Dag goufen déi zwee national Gesetzer am Mémorial A publizéiert: A 225 reegelt NIS-2 zu Lëtzebuerg, an A 226 d'CER-Gesetz. Béid Gesetzer sinn den 10. Mee 2026 a Kraaft getrueden. An interessant ass: Bei béide Gesetzer stinn d'Sécherheetsmoossnamen am Artikel mat där selwechter Nummer, nämlech am Artikel 12!

Moderator (Chris)
Wou verbannen den Artikel 12 vum CER-Gesetz an den Artikel 12 vum NIS-2-Gesetz d'Ufuerderunge mat der Zougangskontroll?

Klaus Wollscheid
Am Lëtzebuerger CER-Gesetz verlaangt den Artikel 12, Paragraf 1, Punkten 2 a 5 – entspriechend dem Artikel 13, Paragraf 1, Buschtawen b an e, vun der europäescher CER-Richtlinn – de physesche Schutz vun den Anlagen an ugepasste Moossname fir d'Personalsécherheet an d'Zougangsrechter. Am Lëtzebuerger NIS-2-Gesetz behandelen den Artikel 12, Paragraf 2, Punkten 8 bis 10 – entspriechend dem Artikel 21, Paragraf 2, Buschtawen h, i an j, vun der EU-Richtlinn – Kryptografie, strikt Zougangskontrollen, d'Sécherung vum physeschen Zougang an eng ugepasst Authentifizéierung. Fir eist Waasserwierk heescht dat ganz konkret: Just autoriséiert Persoune kommen an d'Leitstell, de Server vun der Zougangskontroll ass digital ofgeséchert, entzunne Rechter ginn an enger no Risiko festgeluechter Frist tatsächlech onwierksam, an den Noutbetrib ass duerch Funktiounstester nogewisen.

Moderator (Chris)
Wéi steet et ëm d'Verantwortung vun der Geschäftsleedung an ëm méiglech Sanktiounen?

Klaus Wollscheid
D’Geschäftsleedung huet kloer festgeluechte Flichte fir d’Sécherheet! Ënner NIS-2 heescht et: guttgeheeschen, erméiglechen, iwwerwaachen a léieren. D'Leedung muss d'Zougangskonzept guttgeheeschen, Budget a Ressourcen zur Verfügung stellen, Ausfalltester iwwerwaachen an aus Ofwäichunge léieren. Wann déi gesetzlech Viraussetzunge fir e Verstouss erfëllt sinn, gesäit NIS-2 fir betraffen Ariichtunge Geldstrofe vu bis zu zéng Milliounen Euro oder zwee Prozent vum weltwäite Joresëmsaz vir; fir wichteg Ariichtunge bis zu siwe Milliounen Euro oder 1,4 Prozent. Ënner CER gesäit den nationalen Artikel 19 Geldstrofe vu bis zu 250.000 Euro vir. Dës Geldstrofe fir Ariichtunge bedeiten net automatesch eng perséinlech Haftung vun all eenzelnem Member vun der Geschäftsleedung; dofir gëlle gesondert gesetzlech Viraussetzungen.

Moderator (Chris)
Wéi eng Friste mussen d'Bedreiwer an d'Hiersteller anhalen?

Klaus Wollscheid
Kucke mir d'Zäitlinn un. Den 10. Mee 2026 si CER an NIS-2 zu Lëtzebuerg a Kraaft getrueden. Den 10. Juli 2026 ass d'Frist fir déi éischt Selbstregistréierung ënner NIS-2 ofgelaf. Zanter dem 11. September 2026 gëllen déi éischt CRA-Meldeflichte fir Hiersteller bei aktiv exploitéierte Schwachstellen. Den 11. Dezember 2027 ginn d'Haaptflichte vum EU-Cyber-Resilience-Act, der Veruerdnung 2024/2847, fir digital Produkter uwendbar. Fir Ariichtungen, déi ënner CER benannt goufen, muss zousätzlech bannent néng Méint no der Benennung déi ëmfaassend Risikoanalys virleien; no zéng Méint ginn déi zoutréffend Bestëmmunge vum Kapitel 4 am Prinzip uwendbar, ausser wann eng gesetzlech Ausnam gëllt!

Kapitel 5: De Prinzip vun de Schutzschichten an de Liewenszyklus vun den Zougangsrechter

Moderator (Chris)
Komme mir zum Kär vun der physescher Sécherheetsarchitektur: dem Prinzip vun de Schutzschichten, och Zwiwwelschueleprinzip genannt. Wéi gesäit dëse Modell am Waasserwierk aus?

Klaus Wollscheid
De Zwiwwelschueleprinzip deelt de Standuert a véier Schutzgrenzen an, déi vun dobaussen no bannen anenee leien. Schicht 1 ass den Terrain oder de baussenzege Perimeter: Zonk, Paart, Barrière a Besucherféierung. Schicht 2 ass d'Gebai oder de bannenzege Perimeter: kontrolléiert Baussendieren, déi just berechtegt Persounen eraloossen. Schicht 3 ëmfaasst sensibel Raim: d'Leitstell, de Laboratoire oder de Serverraum, mat eegene rollenofhängegen Zougangsrechter. Schicht 4 schützt déi kritesch Komponenten direkt: e verspaart Steierungsschaf, eng SPS-Steierung oder e Serverrack, dat just mat enger separater Fräigab fir eng konkret Aufgab opgemaach dierf ginn. All passend ausgeleeë Schicht soll onerlaabten Zougang erschwéieren an Zäit fir eng Reaktioun schafen. D’Norm EN 50600-2-5 behandelt Sécherungssystemer fir Rechenzentren; eis véier Schichte sinn hei e Planungsmodell fir d’Waasserwierk, keng allgemeng Normflicht.

Moderator (Chris)
Wéi leeft esou e Wee duerch déi véier Schichten an engem konkrete Fall of, zum Beispill bei engem externen Ënnerhaltstechniker?

Klaus Wollscheid
Huele mir un, en externe Techniker soll haut d'Pompel 3 an der Leitstell waarden. Bei der éischter Schicht, der Paart, gi seng Identitéit a säi Rendez-vous kontrolléiert; um Empfang kritt en eng Zougangskaart. Bei der zweeter Schicht, der Entrée vum Gebai, mécht d'Kaart just während engem begrenzten Zäitraum op. Bei der drëtter Schicht, der Leitstell, gëtt de Responsabele vum Betrib den Zougang fräi, eventuell nëmme mat Begleedung. Bei der véierter Schicht, dem Steierungsschaf, gëtt d'Schlëssel- oder Fräigabbox fir genee dëse Schaf fräigeschalt. Nom Ënnerhalt ginn déi befrist Zougangsrechter no der ofgemaachter Prozedur entzunn, d’Schief ginn erëm verspaart an déi wichteg Schrëtt ginn novollzéibar dokumentéiert!

Moderator (Chris)
Wéi steiert een dës Rechter iwwer de ganze Liewenszyklus vu Mataarbechter an externe Firmen?

Klaus Wollscheid
Mir schwätze vum Liewenszyklus vun den Zougangsrechter, mat dräi Phasen. Éischtens den Entrëtt: Identitéit préiwen, eng Roll am Personalverwaltungssystem festleeën an eng Kaart ausginn. Zweetens eng Ännerung: Wann d'Aufgab oder den Departement wiesselt, ginn déi al Rechter no der festgeluechter Prozedur wierksam entzunn an nëmmen déi néideg nei Rechter verginn. Drëttens den Austrëtt: Wann eng Persoun d'Entreprise verléisst, muss hir Kaart bannent der festgeluechter Frist wierksam gespaart ginn; d’Sperrung muss iwwerpréift an dokumentéiert ginn. Fir bestëmmte sensibel Funktiounen, déi gesetzlech definéiert sinn, kann am Kader vum CER eng formell Personalpréiwung néideg sinn. Esou e Bescheed gëllt am Prinzip fënnef Joer; d’Erneierung muss am gesetzlechen Zäitraum vu sechs bis véier Méint virum Oflaf ugefrot ginn!

Moderator (Chris)
Wat geschitt, wann eng Schicht ausfält oder ëmgaange gëtt?

Klaus Wollscheid
Dat ass den entscheedenden Härtetest! Wann d'Schicht 1, also zum Beispill d'Paart, wéinst enger Stéierung opbleift, sollen déi bannenzeg Schichten 2, 3 a 4 den onerlaabten Zougang weiderhi wierksam begrenzen. Gläichzäiteg soll eng ugepasst Iwwerwaachung zum Beispill erkennen, wann eng Dier vun der Leitstell ze laang opsteet, an eng virdru festgeluecht Reaktioun ausléisen. Och Liwweranten an Niewenentréeë musse passend a kloer dokumentéiert Zougangsreegele kréien.

Kapitel 6: Grenze vun der Mechanik, Stand vun der Technik a Reifegraden

Moderator (Chris)
Vill méi kleng oder méi al Waasserwierker vertrauen nach haut op reng mechanesch Schléissanlagen. Firwat geet dat ënner NIS-2 a CER dacks net méi duer?

Klaus Wollscheid
Reng mechanesch Schlëssele weisen an engem Audit dräi grouss Schwächten. Éischtens d'Nohvollzéibarkeet: E mechanescht Schlass erstellt selwer kee digitalt Evenementsprotokoll. Domat kann een net iwwer d'Schlass nokucken, wien d'Dier wéini opgemaach huet. Zweetens de Verloscht an d'Kopien: Wann e Generalschlëssel verluer geet, kann een en net mat engem Mausklick späre; et muss jee no Schléisshierarchie gekläert ginn, wéi eng Zylinder betraff sinn a wéi eng Ersatzmoossname passen. Drëttens d'Zäit- a Rollesteierung: E mechanesche Schlëssel funktionéiert ronderëm d'Auer a kennt weder Schichtpläng nach befrist Ënnerhaltszäiten.

Moderator (Chris)
NIS-2 verlaangt Moossnamen nom „Stand vun der Technik“. Wat heescht dëse rechtleche Begréff bei der Zougangskontroll?

Klaus Wollscheid
De Stand vun der Technik bedeit: Schutzmoossnamen, déi dem aktuelle Stand vun der technescher Entwécklung entspriechen, fir de konkrete Risiko gëeegent sinn an an der Praxis wierken. D'Virgoensweis huet véier Schrëtt: Éischtens Risiko a Schutzbedarf bestëmmen; zweetens gëeegent Moossnamen op Basis vun Normen auswielen; drëttens hir Wierksamkeet am Betrib testen an noweisen; a véiertens reegelméisseg nei bewäerten. Den Opwand an d'Käschte spille bei der Verhältnisméissegkeet eng Roll, mä den néidege Schutzniveau vun der kritescher Anlag bleift entscheedend!

Moderator (Chris)
Du hues dozou e verständlechen Entwécklungsmodell mat véier Stufen ausgeschafft. Kënns du eis déi véier Reifegrade erklären?

Klaus Wollscheid
Gären. Stuf 01, reaktiv a mechanesch: reng mechanesch Schlëssele, déi manuell registréiert ginn; bei Verloscht muss eventuell d'Schlass ersat ginn. Stuf 02, identifizéiert an elektronesch: Elektronik an RFID-Medien; perséinlech Zougangskaarten erlaben Evenementsprotokoller a geziilt Späre, mee d'Zäit bis zur Wierkung hänkt staark vun der Systemarchitektur of. Stuf 03, dynamesch Rechterverwaltung: ofhängeg vum System automatiséiert Rollen- a Rechterverwaltung, befrist Zäitraim fir den Ënnerhalt an eng automatesch Verbindung mam Personalverwaltungssystem beim Austrëtt. Stuf 04, proaktiv Iwwerwaachung: dem Risiko ugepasst Iwwerwaachung vun ausgewielten Zougangspunkten, wann néideg mat automatescher Erkennung vun Attacken, dem Risiko ugepasste Méifach-Authentifizéierung, zum Beispill Kaart a PIN bei der Leitstell, an e reegelméisseg getestenen Noutbetrib.

Kapitel 7: Systemopbau, Kryptografie an d’Roll vum CRA

Moderator (Chris)
Wa mir eng elektronesch Zougangskontroll installéieren, gëtt dëse System selwer zu engem interessanten Zil fir Cyberattacken. Wéi schütze mir d'Infrastruktur vun der Zougangskontroll?

Klaus Wollscheid
Genee dofir muss och d'Zougangskontroll selwer technesch ofgeséchert ginn! D'Kette besteet aus Kaart, Lieser, Diersteierung an Verwaltungssoftware. Je no Schutzbedarf kënne Manipulatiounskontakter a passend Verrigelungsmechanismen un der Dier néideg sinn. De Server fir d’Zougangskontroll muss no der Risikoanalys ofgeséchert ginn, zum Beispill mat Netzsegmentéierung an enger passender Méifach-Authentifizéierung fir d’Administratioun. Och d’Verbindungen tëscht de Komponenten brauchen eng passend Authentifizéierung a kryptografesch Sécherung!

Moderator (Chris)
Wéi gesäit dës Kryptografie op den dräi Iwwerdroungsstrecke konkret aus?

Klaus Wollscheid
Mir sécheren dräi Strecken of. Streck 1, vun der Kaart zum Lieser: D'Echtheet vun der Kaart gëtt mat verschlësselte Challenge-Response-Verfaren iwwerpréift, zum Beispill MIFARE DESFire, fir Kopien a Replay-Attacken däitlech méi schwéier ze maachen. Streck 2, vum Lieser zum Controller: Noriichten authentifizéieren an de Buskabel géint Manipulatioun schützen, zum Beispill mat OSDP v2 Secure Channel. Streck 3, vum Controller zum Server: Géigesäiteg Zertifikatskontroll a verschlësselt Netzwierkiwwerdroung. Fir Audite ganz wichteg: Et gëtt keng steif Flicht, un all Dier AES-256 oder TLS 1.3 ze benotzen. D'Verfare musse passend zum Risiko gewielt an an de Liewenszyklus vum Schlësselmanagement agebonne ginn!

Moderator (Chris)
Wéi eng Roll spillt hei den neien EU-Cyber-Resilience-Act, de CRA?

Klaus Wollscheid
De CRA, d'EU-Veruerdnung 2024/2847, leet de Produkthiersteller Flichten op. Fir Produkter, déi ënner de CRA falen, mussen d’Hiersteller vu Lieser, Controlleren a Software fir d’Zougangskontroll passend sécher Standardastellungen ubidden, Schwachstellen am zoutréffende Supportzäitraum behandelen a Sécherheetsupdates liwweren. De CRA gesäit am Prinzip mindestens fënnef Joer Support vir, ausser wann déi erwaart Notzungsdauer méi kuerz ass; bei enger méi laanger Notzung kann e méi laange Supportzäitraum néideg sinn. Bei der Iwwergab vum Produkt verbënnt den Akaf den Hiersteller mam Bedreiwer: De Bedreiwer iwwerhëlt déi sécher Konfiguratioun, an den Hiersteller stellt déi gesetzlech erfuerderlech a vertraglech ofgemaach Support- an Updateweeër zur Verfügung.

Kapitel 8: Déi dräi praktesch Auditfäll am Detail

Moderator (Chris)
Elo komme mir bei dee spannendsten Deel fir Auditeuren a Sécherheetsverantwortlech aus der Praxis: déi dräi praktesch Auditfäll am Waasserwierk! Fänke mir mam éischte Fall un: E Mataarbechter verléiert seng Zougangskaart. Wat geschitt?

Klaus Wollscheid
Deen éischte Fall weist den Ënnerscheed tëscht Online- an Offline-Dieren! De Mataarbechter mellt de Verloscht, an d'Kaart gëtt am zentrale System gespaart. Bei der Online-Dier vun der Leitstell kann d'Spär séier wierken, wann d’Verbindung funktionéiert. Entscheedend ass, datt de Controller d’Ännerung iwwerhëlt an d’Dier déi gespaart Kaart tatsächlech ofweist. Bei der ofgeleeëner Offline-Dier vun der Pompelstatioun gëtt et awer keng permanent Verbindung. Do hänkt d’Wierkung vun der Spär zum Beispill dovun of, wéini aktualiséiert Spärdaten lokal ukommen oder eng zäitlech limitéiert Berechtegung ofleeft. Fir den Audit heescht dat: Déi maximal zoulässeg Spärzäit muss am Viraus an der Risikoanalys festgeluecht an um richtege Schlass nogewise ginn, och bei engem simuléierten Netzausfall!

Moderator (Chris)
Wéi gesäit den zweete Fall aus: e komplette Stroum- oder Netzwierkausfall am Waasserwierk?

Klaus Wollscheid
Deen zweete Fall betrëfft den Noutbetrib! Wann d'Netzwierkverbindung ausfält, däerfen d'Diercontrolleren net einfach all Dieren ouni Berechtegung fräiginn. Si sollen no der virgesinner Ausleeung mat lokal gespäicherte Rechter a Spärreegele sécher weiderfunktionéieren. Bei engem Stroumausfall muss déi néideg Autonomie oder eng passend Ersatzprozedur virgesi sinn. Besonnesch wichteg: Sécher Flucht, Schutz géint onerlaabten Zougang an Noutöffnung musse fir all Dier no den zoutréffende Bau- a Brandschutzreegelen ofgestëmmt a getest ginn. Berechtegt Betribspersonal muss d'Anlag trotzdeem iwwer definéiert Noutzougäng erreeche kënnen. Wann de Stroum zeréckkënnt, mussen d'Evenementer an d'Zäitstempelen kontrolléiert ofgestëmmt ginn.

Moderator (Chris)
An den drëtte Fall verbënnt déi zwee Szenarie bei enger gemeinsamer Ausfallübung. Wéi leeft dëse Stresstest zäitlech of?

Klaus Wollscheid
Bei der Auditübung simuléiere mir dräi Phasen. Um 08:10 Auer fält d'Netz aus, an en Techniker muss an d'Leitstell kommen. D'Resultat: Den Noutzougang gëtt iwwerpréift, an déi virgesinne Fluchtfunktioune ginn am Test nogewisen. Um 08:20 Auer mellt e Mataarbechter de Verloscht vun enger Kaart. Bei der offline bedriwwener Pompelstatioun ass d'Recht nach um Medium gespäichert. D'Resultat: De Restrisiko gëtt duerch virdru festgeluecht organisatoresch Ersatzmoossnamen effektiv begrenzt. Um 08:35 Auer kënnt de System zeréck. D'Resultat: Déi lokal gespäichert Zougangsevenementer ginn am Kader vun de Systemméiglechkeete kontrolléiert ofgestëmmt. Bei engem méigleche Produktfeeler gëtt den Hiersteller agebonnen; ob eng gesetzlech CRA-Meldung néideg ass, muss déi jeeweils verflicht Persoun oder Organisatioun separat préiwen. Dës Übung liwwert wichteg Nofweiser fir déi betriblech Resilienz!

Kapitel 9: Meldeflichten a zoustänneg Stellen: 24 Stonnen, 72 Stonnen, ee Mount

Moderator (Chris)
Wann e schwéiere Virfall geschitt, zum Beispill eng Sabotage un der Zougangskontroll, déi de Betrib vum Waasserwierk stéiert, kënnen streng gesetzlech Meldeflichten entstoen. Wéi ënnerscheede sech d'Meldeweeër ënner NIS-2, CER a CRA?

Klaus Wollscheid
Dat ass eng vun de komplizéiertste Froen an der Praxis, well een eenzege Virfall gläichzäiteg zwou verschidde gesetzlech Meldeweeër ausléise kann! Kucke mir d'Fristen un. Ënner NIS-2, bei erhebleche Sécherheetsvirfäll: Éischtens eng Fréiwarnung bannent 24 Stonnen, nodeems de Virfall bekannt ass. Zweetens d'Virfallmeldung bannent 72 Stonnen. Drëttens en obligatoreschen Ofschlossbericht ee Mount no der Virfallmeldung. Ënner CER, bei erhebleche Stéierunge vun der Resilienz: Éischtens eng éischt Meldung bannent 24 Stonnen no der Kenntnisnam; zweetens en detailléierten Ofschlossbericht bannent engem Mount. Bei CER gëtt et kee generelle weidere Schrëtt no 72 Stonnen! Fir CER ass den Haut-Commissariat à la Protection Nationale, HCPN, zoustänneg; fir NIS-2 den ILR, respektiv am Finanzsecteur d'CSSF. D'CRA-Meldunge vun Hiersteller iwwer Schwachstelle lafen iwwer separat Weeër mat ENISA an den nationale CSIRTen.

Kapitel 10: Den Ëmsetzungsplang iwwer 90 Deeg a véier Decisioune fir d’Leedung

Moderator (Chris)
Wéi kënne mir all dës Ufuerderungen dauerhaft am Informatiounssécherheetsmanagementsystem, dem ISMS, verankeren?

Klaus Wollscheid
Mir recommandéieren en zouene Kreeslaf am ISMS mat véier Schrëtt: Risiko erkennen, Moossnam festleeën, d'Wierksamkeet am Betrib noweisen a kontinuéierlech verbesseren. Fir en Audit ass déi gesammelt Dokumentatioun wichteg: Zoneplang, Iwwerpréiwung vun den Zougangsrechter, Konfiguratiounsnofweiser, Ënnerhaltsprotokoller, Virfallsberichter a Protokoller vun den Noutfallübungen. En héije, gutt dokumentéierte Reifegrad hëlleft bei der Opsiicht staark, mä et gëtt keng automatesch Befreiung vun engem Audit!

Moderator (Chris)
Wéi gesäit fir Bedreiwer, déi elo mussen ufänken, e pragmateschen Ëmsetzungsplang iwwer 90 Deeg aus?

Klaus Wollscheid
Mir deelen déi éischt 90 Deeg an dräi kloer Phasen vu jee 30 Deeg an. Dag 01 bis 30, anuerdnen an erfaassen: Betroffenheet a Registréierung klären, Zonen, Anlagen an Déngschtleeschter erfassen, d'Schlëssel- a Berechtegungslëschten zesummeféieren. Dag 31 bis 60, Lücke schléissen: d'Risikoanalys maachen, Prioritéite festleeën, gëeegent Zougangstechnologie a Spärprozesser auswielen, Noutzougäng virgesinn an d'Zousoe vun den Hiersteller am CRA-Kontext kréien. Dag 61 bis 90, testen a verankeren: Ausfall- an Neistarttester un de richtegen Dieren duerchféieren, Personal schoulen, Nofweiser zesummestellen an de System am ISMS verankeren.

Moderator (Chris)
Zum Ofschloss vum Haaptdeel: Wéi eng véier zentral Decisioune soll d'Geschäftsleedung elo treffen?

Klaus Wollscheid
Et si genee véier Decisiounen. Éischtens de Schutzbedarf bestätegen: fir d'Drénkwaasserversuergung, d'Zonen an déi maximal toleréierbar Ausfallzäite verbindlech Ziler festleeën. Zweetens d'Verantwortung verbannen: d'Geschäftsleedung, de Betrib, d'IT, de Personalberäich an extern Liwweranten un een Dësch bréngen. Drëttens d'Zougangskonzept guttgeheeschen: déi néideg Budgete fir d'Entzéie vu Rechter, den Noutbetrib, d'Kryptografie an den Hierstellersupport zur Verfügung stellen. Véiertens d'Wierksamkeet beweisen: e gemeinsamen prakteschen Ausfalltest plangen an d'Nofweiser am Audit bewäerten. CER an NIS-2 leeden de Programm, an de CRA stäerkt d'Produkter, déi dofir agesat ginn!

Kapitel 11: Vertiefungen: DORA, speziell Reegele an technesch Themen

Moderator (Chris)
Klaus, an der Presentatioun hu mir nach zwielef Reservefolien mat ganz wäertvollem Fachwëssen. Loosst eis déi wichtegst Punkte fir Fachleit kucken. Wéi hänke NIS-2, de Finanzsecteur an DORA zesummen?

Klaus Wollscheid
An der Reservefolie R4 gëtt dat kloer erkläert. Fir betraffe Finanzinstitutioune kann d’DORA-Veruerdnung als speziell Reguléierung gëllen; Iwwerschneidunge mat NIS-2 sinn jee no Flicht an Ariichtung ze préiwen. D’CSSF iwwerwaacht déi Finanzberäicher, déi hir gesetzlech zougewise sinn. Bei CER an NIS-2 hänken d’Zoustännegkeete vun der Ariichtung an der jeeweileger Reguléierung of, ënner anerem beim HCPN an ILR.

Moderator (Chris)
Wéi ënnerscheet de Cyber Resilience Act d'Produktkategorie bei Zougangskontrollsystemer?

Klaus Wollscheid
D'Reservefolie R6 weist dräi Gruppen. Kategorie 01, d'Basiskategorie: allgemeng digital Produkter. Kategorie 02, wichteg Produkter nom Annexe III, Klassen I an II: dozou gehéieren d'Verwaltung vun Identitéiten a privilegéierten Zougäng, IAM/PAM, an och verschidde Smart-Home- a Sécherheetsschlässer. Kategorie 03, kritesch Produkter nom Annexe IV: spezifesch héichkritesch Komponenten. Wichteg ass: E Produkt gëtt net eleng doduerch zu engem kritesche CRA-Produkt, datt et an enger kritescher Infrastruktur agesat gëtt. Entscheedend ass seng Haaptfunktioun!

Moderator (Chris)
Wéi eng Krittäre recommandéiert EIWTC fir d'technesch Ofnam vun enger Zougangskontroll?

Klaus Wollscheid
D'Reservefolie R7 bitt eng Checklëscht mat fënnef Punkten. Éischtens Identitéit a Berechtegung: eendeiteg Identifikatioun vun de Geräter an en erfollegräiche Spärtest. Zweetens geschützt Kommunikatioun: authentifizéiert a verschlësselt Bus- an Netzwierkverbindungen. Drëttens Firmware an Updates: signéiert Firmware an en erfollegräichen Negativtest mat net autoriséierten Updates. Véiertens Schlësselen an Zertifikater: gereegelt Prozesser fir Erneierung, Widderruff an Ersatz am Noutfall. Fënneftens Disponibilitéit a Support: nogewisenen Noutbetrib an eng schrëftlech Supportzouso vum Hiersteller fir déi no CRA an erwaarter Notzung zoutrëffend Dauer.

Moderator (Chris)
Wéi eng Roll spillt déi zivil a militäresch Verdeedegung am Kader vun der nationaler Resilienzstrategie, der SNR?

Klaus Wollscheid
D'Reservefolie R9 betount: National Resilienz brauch ofgestëmmt Verantwortung! De strategeschen nationale Resilienzkader gesäit Resilienzbeoptraagter a Kontinuitéitspläng an allen ëffentlechen Institutioune vir. E Waasserwierk kann eng wichteg Roll fir déi national Krisevirbereedung spillen an, ofhängeg vun den tatsächlechen Aufgaben, fir weider staatlech Funktioune relevant sinn. Krisekontakter a Pläng fir de Neistart solle mat de jeeweils zoustännege Stelle jee no konkret festgeluechter Verantwortung ofgestëmmt ginn.

Moderator (Chris)
Klaus, dat war eng fantastesch, ëmfaassend an detailléiert Rees duerch all d'Facette vun der Cyber- a Sabotagesécherheet fir kritesch Infrastrukturen! Villmools Merci fir dat fundéiert Fachwëssen an déi kloer Tipps aus der Praxis.

Klaus Wollscheid
Ganz gären, Chris! Villmools Merci, a vill Erfolleg un all Bedreiwer bei der Ëmsetzung!