Cyber Resilience Act – Transkriptioun vum Podcast

Audio op Däitsch · Transkriptioun op Lëtzebuergesch · 26:05

Lëtzebuergesch Iwwersetzung vum däitsche Gespréich, mat Zäitmarken a liicht fir d’Liesen iwwerschafft. An de fachlechen Erklärunge fannt Dir Prezisiounen zu e puer vereinfacht Aussoen aus der Opnam.

Fachlech Erklärungen zum Gespréich

Fachlech Erklärunge vum 15. November 2026.

Ënnerstëtzung an Aktualiséierungen. De Support muss am Prinzip op d’mannst fënnef Joer daueren. Wann d’Benotzungsdauer vum Produit viraussiichtlech méi kuerz ass, kann de Support op déi erwaart Dauer begrenzt ginn. Automatesch Sécherheetsupdates si virgesinn, souwäit dat op de Produit zoutrefft.

Software-Stécklëscht. D’SBOM muss op d’mannst déi direkt Ofhängegkeeten op der éischter Stuf enthalen. D’Flicht, d’Komponenten ze dokumentéieren, gëtt net all Keefer automatesch d’Recht op déi komplett SBOM.

Meldungen. Den Artikel 14 gëllt zënter dem 11. September 2026. Wann den Hiersteller gewuer gëtt, datt eng Sécherheetslück aktiv ausgenotzt gëtt oder datt et e schwéiere Sécherheetsvirfall gouf, muss hien am Prinzip bannent 24 Stonnen eng éischt Warnung ofginn. Déi nächst Meldung muss bannent 72 Stonne vun deem Zäitpunkt un nokommen. D’Frist fir de Schlussrapport hänkt vum Fall of.

Produkthaftung. Den EU-Rechtsakt 2024/2853 ass eng Richtlinn. Wann en Update feelt, kann dat eng Roll bei der Fro spillen, ob e Produit feelerhaft ass. Et muss och e Schued entstane sinn, fir deen et eng Entschiedegung ka ginn, an dee Schued muss op de Feeler zeréckzeféiere sinn. Schied u Saachen an Donnéeën, déi ausschliisslech berufflech benotzt ginn, falen net ënnert dës Richtlinn.

CE-Markéierung. Den Artikel 30, Abschnitt 4, vum CRA verlaangt, datt d’Kennnummer vun der notifizéierter Kontrollstell hannert dem CE-Zeeche steet, wann déi Stell un der Konformitéitsbewäertung mat ëmfaassender Qualitéitssécherung nom Modul H bedeelegt ass.

(EU) 2024/2847 · (EU) 2024/2853 · Meldepflichten am CRA

De vernetzte Babyphone an de Geltungsberäich

00:00 Stell der emol vir, du keefs dir e fonkelneien Auto, jo? – Jo, okay. – E schéinen neien Auto. – Genee. Du fiers beim Händler vum Haff, gëss op der Autobunn Gas, bis op 130 Kilometer an der Stonn, an op eemol mierks de, datt den Hiersteller einfach d'Bremsen vergiess huet. – Dat wier éischter ongënschteg, jo. – An ob! Du riffs also a Panik beim Clientsservice un, an do seet een dir ganz gemittlech: „O, pardon! D'Bremsbeläg musst Dir Iech selwer am Internet eroflueden an iergendwéi abauen. Vill Gléck dobäi!" – Dat kléngt dach komplett absurd. – Richteg. – Jidderee géif direkt kloen. – Richteg.

00:34 An der digitaler Welt keefs de praktesch all Dag intelligent Dierschlässer, Babyphonen oder WLAN-Router, bei deene genee dat geschitt. – Jo, leider. Et keeft een e Produit, deen nach net fäerdeg ass. – Genee. En onfäerdegen, onséchere Produit, an als Keefer dréis du de ganze Risiko. Op jidde Fall bis elo. D'EU zitt nämlech elo d'Noutbrems. An dat mat enger Kraaft, déi ee sech kaum virstelle kann. Dat wäert déi ganz Techindustrie weltwäit richteg duercherneerëselen. – Gutt gesot.

01:06 An domat häerzlech wëllkomm bei eiser Analyse vun haut. Flott, datt s du als drëtt Persoun an eiser Ronn nees dobäi bass. Schéin, datt s de nolauschters. Mir kucken eis haut eppes un, wat op den éischte Bléck no dréchener Bréisseler Bürokratie kléngt. – Ass et dat dann? – Nee, guer net. A Wierklechkeet ass dat en Äerdbiewe fir d'Reglementatioun. Mir schwätze vum neien EU-Reglement 2024/2847, besser bekannt als den europäesche Cyber Resilience Act, kuerz CRA. – Genee. Eis eenzeg Quell haut ass den Originaltext vun der EU. Keng Panik, mir maachen dat Ganzt fir dech verständlech. – Da kucke mer eis dat emol méi genee un.

01:47 Jo, leeë mer lass. Fir dat gräifbar ze maachen, hunn ech geduecht, mir erfannen haut e Produit, mat deem mir déi nei Reegelen duerchspillen. Nenne mer en de Smart Baby 3000. – Smart Baby 3000, dat gefält mer. Wat kann deen? – Dat ass e ganz moderne Babyphone mat WLAN, HD-Kamera an enger Cloud-App fir däi Smartphone. Mat allem, wat dozougehéiert. – A wat ännert sech duerch de CRA fir genee dësen Apparat? – Fir dat ze verstoen, musse mer fir d'éischt kucken, wat dat neit Reglement ofdeckt.

02:19 De CRA gëllt fir all, an elo zitéieren ech, „Produite mat digitalen Elementer". – Dat kléngt immens breet. – Dat ass et och. Am Text geet et ëm Produiten, déi hirem Zweck no eng direkt oder indirekt, logesch oder physesch Dateverbindung mat engem Apparat oder engem Netzwierk hunn. – Da fält eise Smart Baby 3000 voll drënner. – Zu honnert Prozent, well en Hardware a Software verbënnt a fir seng Funktioun vernetzt ass. Ausgeholl sinn am Fong just déi Beräicher, an deene schonn immens streng speziell Virschrëfte gëllen. – Also zum Beispill medezinesch Apparater oder Fligeren. – Genee, fir Autoen, an der Loftfaart an an der Medezin gëtt et schonn haart Reegelen.

02:57 Waart emol. De Babyphone selwer steet bei mir am Kannerzëmmer. Mee wéi ass et mat der App an der Cloud? – Dat ass eng ganz gutt Fro. – D'Videosignal leeft dach dacks iwwer e Server iergendwou am Ausland. Regelt d'EU just d'Plastiksgehäis an de Chip oder fält d'Cloud och drënner?

03:17 Dat ass eng ganz wichteg Ënnerscheedung. Am Prinzip regelt de CRA Produiten. Reng Servicer falen net drënner. Et gëtt awer e groussen „Awer“. Wann esou eng Dateveraarbechtung aus der Distanz, also an der Cloud, néideg ass, fir datt de Produit iwwerhaapt seng Funktioun erfëllt, fält se ënnert de CRA. – Ah, okay. – Wann däi Smart Baby 3000 ouni d’Schnittstell um Server vum Hiersteller kee Bild op däin Handy kritt, ass dës Cloud-Komponent juristesch gesinn en Deel vum gereegelte Produit. – Oha! Den Hiersteller kann sech also net domat erausrieden: „Eisen Apparat ass sécher, et gouf leider just dee Server do gehackt.“ – Genee, dat gëllt net méi. Hien haft fir dat Ganzt.

Sécher Astellungen a Verantwortung an der Liwwerketten

03:54 Dat liicht mer an. Mee wat genee verlaangt d’EU? Däerf een den Apparat einfach op de Marché bréngen a spéider, wann Hacker iwwer de Babyphone mat grujelege Stëmmen an d’Kannerzëmmer ruffen, e Patch noliwweren? – Dat geet elo net méi. Domat ass Schluss. Am Mëttelpunkt vum Reglement steet „Security by Design and Default“. – Also Sécherheet vun Haus aus. – Jo, genee. Bis elo huet een dacks eréischt duerno un d’Sécherheet geduecht. Esou wéi e Plooschter, deen een op eng oppe Wonn pecht. – Nom Motto: „Mir flécken dat herno nach.“ – Richteg. D’Gesetz verflicht d’Hiersteller elo, Produiten ouni bekannt, ausnotzbar Sécherheetslücken op de Marché ze bréngen. Dat gëllt schonn um Zeechebriet. – Wow!

04:33 Dozou gehéiert och, sou mann Donnéeë wéi méiglech ze sammelen. De Babyphone däerf also net heemlech iergendwellech Metadate fir Reklamm sammelen, wann déi fir säi Fonctionnement guer net néideg sinn. – Dat ass bei engem Babyphone wierklech berouegend. – Jo, gelldu? A virun allem muss de Schutz géint onerlaabten Zougréff par défaut ageschalt sinn. – Dat heescht, dës berüchtegt Standardpasswierder wéi „Admin 123“ oder einfach „0000“, déi fréier op Milliioune Geräter fest programméiert waren, sinn dann illegal? – Absolutt. All Apparat muss eege Zougangsdonnéeën hunn. Oder e muss dech forcéieren, beim éischten Aschalten e wierklech séchert Passwuert festzeleeën. – Endlech!

05:13 Faszinéierend ass och de wirtschaftlechen Aspekt. D’EU gräift hei an, fir e klassescht Maartversoen ze korrigéieren. – Wéi mengs de dat? – D’Informatioun ass ongläich verdeelt. – Genee. Als normale Benotzer kanns du d’Sécherheet vun esou engem komplexe Smart-Home-Apparat dach guer net aschätzen. – Nee, absolut net. En ass schéin a funktionéiert. – Richteg. Mee ob de Code am Hannergrond ausgesäit wéi e Schwäizer Kéis, dat gesäis du net. Den Hiersteller weess et natierlech. Hien hat awer bis elo kee finanziellen Ureiz, Suen an déi onsichtbar Sécherheet ze stiechen. – Kloer, e schéint Gehäis verkeeft sech besser wéi gutt geschriwwene Code. – Genee. De CRA verlagert déi wirtschaftlech Laascht elo däitlech op den Hiersteller.

05:54 Gutt, deen, deen den Apparat baut, muss investéieren. Mee soe mer emol éierlech: Esou e Babyphone gëtt dach meeschtens iergendwou an Asie produzéiert. – Dacks, jo. – Eng kleng Importfirma bréngt en an Europa an herno läit en hei am Regal vun engem grousse Fachgeschäft fir Elektronik. Wann den Hiersteller an Asie seet: „D’EU-Reegele sinn mir egal“, wat da? Sinn d’Händler an Europa aus dem Schneider? –

Nee, guer net. D’EU huet aus fréiere Reglementer geléiert a bezitt elo déi ganz Liwwerketten an. – Also och d’Elektrogeschäft ëm den Eck?

06:27 Jo. D’Importateuren an d’Händler an der EU si matverantwortlech. Wann s du als grousst Geschäft déi bëlleg Smart-Home-Geräter containerweis aus dem Ausland akeefs, däerfs de se nëmme verkafen, wa se d’CE-Markéierung droen an ee beleeë kann, datt d’IT-Sécherheet an der Rei ass. – Den Händler muss dat also kontrolléieren? – Genee. Huet en och nëmmen e Grond fir unzehuelen, datt dëse Smart Baby 3000 e Risiko duerstellt, däerf en de Babyphone guer net an de Regal stellen. Hie muss de Verkaf stoppen an direkt d’Autoritéiten informéieren.

Open Source a kommerziell Notzung

06:55 Do muss ech awer anhaken. An der Theorie kléngt dat gutt, mee passt dat iwwerhaapt zu der Realitéit an der Softwareentwécklung? – A wéi engem Sënn? – Bal all moderne kommerzielle Produit besteet haut zum Deel aus Open-Source-Komponenten. Den Hiersteller vu mengem Smart Baby 3000 schreift säi Betribssystem dach net vun Ufank u selwer. – Dat stëmmt. – Hien hëlt eng fräi Linux-Versioun, setzt eng Open-Source-Bibliothéik fir d’Kamera vu GitHub drop, a fäerdeg. Wann dee fräie Code, dee Fräiwëlleger geschriwwen hunn, elo onsécher ass, wien haft dann?

07:26 Ech verstinn, wou s de hiwëlls. – Dat kléngt jo, wéi wann dat Gesetz der ganzer fräier Entwécklerszeen géif de Krunn zoudréinen. Wann ech de Weekend a mengem Keller e flotte Smart-Home-Plugin programméieren an e klenge Patreon-Link op meng Säit setzen, fir datt d’Leit mer e Kaffi spendéiere kënnen, kann da géint mech op Millioune geklot ginn, wa mäi Code gehackt gëtt? Well éierlech gesot, wann dat esou ass, huelen ech mäi Code nach haut vum Netz. – Ganz roueg, huel emol déif Loft. Du kanns däi Code roueg online loossen. – Puh, wat e Gléck! – Mee du schwätz do eppes un. Genee dat huet der Open-Source-Gemeinschaft am meeschte Suerge gemaach, wéi déi éischt Entwërf erauskoumen. – Dat kann ech verstoen. – Absolutt.

08:03 Wa mer eis den Text méi genee ukucken, besonnesch d’Erwäägungsgrënn 17 bis 19, gesi mer, wéi elegant de Gesetzgeber dat geléist huet. De CRA mécht e kloren Ënnerscheed tëschent der Entwécklung an der kommerzieller Bereetstellung. – Wat heescht dat genee? – Fräi an quelloppe Software, kuerz FOSS, fält nëmmen ënnert déi streng Flichten, wa se am Kader vun enger kommerzieller Aktivitéit bereetgestallt gëtt. – A mäi Patreon-Knäppche fir de Kaffi? – Dat ass keng kommerziell Aktivitéit. Spenden ouni Gewënnzweck sinn am Gesetz ausdrécklech als Ausnam virgesinn. – Ganz gutt.

08:38 Kommerziell gëtt et eréischt, wann s de mat der Software aktiv Sue verdéngs, zum Beispill andeems de technesch Ënnerstëtzung géint Bezuelung ubitts. Oder, an dat ass fir eng Entreprise de wichtege Punkt, wann s de als grouss Firma de gratis Code vun engem Hobbyentwéckler hëls an en an däi Router oder Babyphone anbaus, deen s de mat Gewënn verkeefs. Dann, a just dann, haft s du als Hiersteller vum fäerdege Produit voll fir d’Sécherheet vun all deenen Open-Source-Bausteng. – Dat ass clever. Den Hiersteller vum Smart Baby 3000 ka sech net méi domat erausrieden, datt de Feeler an der fräier Kamerabibliothéik louch. – Genee. Hie verdéngt Sue mam Gesamtpak an dofir muss hien och dofir astoen, datt déi gratis Deeler, déi en agebaut huet, sécher sinn. –

Dat schützt d’Iddie vun de klengen Entwéckler an hëlt déi grouss Techfirmen an d’Flicht. Flott geléist.

09:31 Mee waart emol, wéi ass et mat de ganz groussen Open-Source-Stëftungen? – Du mengs esou eppes wéi d’Apache Foundation? – Jo. Déi stelle Software hier, mat där gefillt den hallwen Internet leeft. Dacks schaffen dës Stëftungen awer ouni Gewënnzweck. Fir si féiert de Gesetzgeber eng nei Roll an, déi sougenannt „open-source software stewards“, also Organisatiounen, déi quelloppe Software betreien. – Dat kléngt ganz formell. – Dat ass et och. Et si juristesch Persounen, déi Open Source systematesch a laangfristeg ënnerstëtzen, ouni wéi e klasseschen Hiersteller fäerdeg Produiten ze verkafen. – A firwat eng eege Roll?

10:09 Well d’EU verstanen huet: Wann een enger Stëftung wéi Apache Geldstrofe vu Milliounen operleet, da brécht muer den Internet zesummen. Dofir hunn déi Organisatioune vereinfacht Flichten. – Si ginn also e bësse geschount? – Esou ongeféier. Si brauchen eng dokumentéiert Strategie fir d’Cybersécherheet a musse professionell mat Sécherheetslücken ëmgoen. – Dat ass kloer. – Mee si däerfen zum Beispill keng CE-Markéierung ubréngen, an den Text schützt si ausdrécklech virun héije Geldstrofen. Et wëll ee se jo net an de Ruin dreiwen. – Jo, dat ass verständlech. Mir hunn elo also den Design an déi ganz Entwécklungsphas gekläert.

Aktualiséierungen, Ënnerstëtzung a Software-Stécklëscht

10:44 Mee loosse mer emol kucken, wat nom Kaf geschitt. – Gären, d’Zäit, an där de Produit benotzt gëtt. – Genee. Ech benotze mäi Smart Baby 3000 elo zënter dräi Joer. Op eemol entdeckt e Fuerscher am Beräich IT-Sécherheet eng grouss Sécherheetslück an där Kamerabibliothéik. – De klassesche Fall. – Bis elo huet den Hiersteller dacks gesot: „De Modell ass al. Kaaf der dach deen neie Smart Baby 4000.“ Wéi regelt de CRA d’Aktualiséierungen? – Hei gëtt et fir vill Hiersteller wierklech batter. De CRA schreift nämlech e garantéierten Zäitraum fir den technesche Support vir.

11:17 En Zäitraum fir de Support? – Jo. An där Zäit musse Sécherheetsupdates zur Verfügung gestallt ginn. D’Dauer muss där Zäit entspriechen, wärend där de Produit viraussiichtlech benotzt gëtt, an am Prinzip muss se op d’mannst fënnef Joer bedroen. – Fënnef Joer? An der Technologiewelt ass dat eng hallef Éiwegkeet! – Eng Ausnam gëtt et, wann d’Liewensdauer vum Produit vu virera vill méi kuerz ass, zum Beispill bei enger temporärer App fir en Evenement. Bei engem physeschen Apparat schwätze mer an der Reegel vu mindestens fënnef Joer.

11:48 A kommen déi Updates vun eleng oder muss ech dauernd duerch onverständlech Menüe goen an op „No Updates sichen“ klicken? – Dat ass dee nächste grousse Schrëtt. D’Gesetz verlaangt, datt d’Produiten esou entwéckelt ginn, datt Sécherheetsupdates an der Standardastellung automatesch erofgelueden an installéiert ginn. – Yes! – Natierlech muss de dat einfach kënnen ausschalten, falls de et aus iergendengem Grond wierklech net wëlls. Mee als Standard ass et automatesch. An eng aner Virgab fannen ech nach méi interessant: Aktualiséierunge fir nei Funktioune sollen an Zukunft vun de Sécherheetsupdates getrennt ginn. – O, merci, léif EU! Ech muss dann net méi eng

komplett nei Uewerfläch fir d’App installéieren, déi mer de Späicher voll mécht, just fir eng kleng Sécherheetslück zouzemaachen. – Genee. D’Sécherheetsarchitektur gëtt dovun entkoppelt. – Dat ass wierklech praktesch fir d’Benotzer.

12:36 Elo kënnt awer déi richteg Hellenaarbecht fir d’Hiersteller. – Wéi eng? – Wéi soll den Hiersteller vum Smart Baby 3000 no dräi Joer iwwerhaapt nach wëssen, datt genee déi dräi Joer al Open-Source-Bibliothéik déif a sengem Code stécht, déi een elo ugräife kann? – Do kënnt déi Ofkierzung an d’Spill, bei där de Leit aus der IT-Branche grad waarm gëtt: SBOM, richteg? – Genee. SBOM steet fir „Software Bill of Materials“. Op Däitsch seet een „Software-Stückliste“, also eng Lëscht mat de Bestanddeeler vun der Software. De CRA verflicht d’Hiersteller, eng maschinneliesbar Lëscht mat alle Komponenten, Bibliothéiken an Ofhängegkeeten an hirem Produit ze féieren an aktuell ze halen.

13:16 Op den Alldag iwwerdroen ass dat ewéi d’Lëscht mat den Zoutate vun engem Liewensmëttel, oder? – Genee. Wie géint Erdnëss allergesch ass, dréit d’Verpakung ëm a kuckt no, ob Erdnëss dra sinn. Wann elo an engem bestëmmten Deel vum Code eng Sécherheetslück opdaucht, kuckt den Hiersteller a seng SBOM, seng Zoutatelëscht, a mierkt direkt: „Mëscht, dee Code mat der Lück stécht an eisem Babyphone! Mir mussen direkt e Patch erausbréngen.“ – E gudde Verglach. Mee stell der vir, op där Lëscht stinn honnertdausende Saachen, an e puer Zoutate bestinn nees aus Dose vun aneren Zoutate vu Fournisseuren, déi s de net emol perséinlech kenns. – Dat kléngt no engem Albdram.

13:55 Dat ass et och. Mee wa mer dat Ganzt kucken, verstinn ech, firwat eng SBOM esou vill ännert. Erënners de dech u Log4j? – O jo! – Dat war eng kleng Java-Bibliothéik fir ze protokolléieren, wat eng Software mécht. Déi war praktesch iwwerall agebaut. Wéi do eng Sécherheetslück fonnt gouf, war weltwäit Panik. Grouss Konzerner hunn e puer Woche gebraucht, fir iwwerhaapt erauszefannen, a wéi enge vun hiren eegene Systemer Log4j gelaf ass. – E risege Päiperlekseffekt. – Genee. Mat enger SBOM kanns de deng Stécklëschten automatesch duerchsichen an du weess a Brochdeeler vun enger Sekonn, wéi eng vun denge Produite betraff sinn. Dat hanneno fir ale Code opzebauen ass logistesch immens schwéier. Fir d’Zukunft ass et awer onverzichtbar.

Produktrisiko, Konformitéit an CE-Kennzeechen

14:35 Wow! Mir hunn elo also e sécheren Design, fënnef Joer laang automatesch Updates an eng komplett Zoutatelëscht. Mee wie kontrolléiert dat alles? Vertraut d’EU einfach op d’Hiersteller? Ännert sech eppes op der Verpakung vu mengem Babyphone? – Déi Markéierung, déi een op der Verpakung gesäit, bleift d’CE-Markéierung. Hir Bedeitung ännert sech awer däitlech. – A wéi engem Sënn? – Bei villen intelligente Geräter stoung d’CE-Zeeche bis elo dacks just fir elektresch Sécherheet, zum Beispill dofir, datt den Netzdeel net a Brand geréit, oder fir bestëmmte Funknormen. Vun elo u steet et zwéngend och fir IT-Sécherheet nom CRA. – A wie préift dat?

15:17 Dat hänkt vun der Risikoklass of. Bei de sougenannte Standardprodukte mat niddregem Risiko däerf den Hiersteller d’Konformitéit nach an engem interne Kontrollverfare selwer bewäerten an dokumentéieren. – Mee mäi Smart Baby 3000 huet

eng Kamera, déi direkt a mäi Kannerzëmmer filmt. Dat ka kee Standardrisiko sinn, oder? – Ganz richteg. Esou Produite falen an d’Kategorie vun de wichtege Produite mat digitalen Elementer. Déi sinn nach eng Kéier a Klass 1 a Klass 2 agedeelt. – Wat fält a Klass 1? – Zum Beispill intelligent Haushaltsapparater mat Sécherheetsfunktiounen, Babyphonen, vernetzte Spillsaachen oder Passwuertmanager. Wann en Hiersteller do net strikt no den harmoniséierten EU-Norme schafft, muss zwéngend eng onofhängeg Kontrollstell dat préiwen.

15:59 A wou gesinn ech dat als Keefer? – Dann steet niewent dem CE-Zeechen och déi véierstelleg Kennnummer vun där Kontrollstell. – Verstinn. A Klass 2? – Dat sinn nach méi sensibel Saachen: Firewalls, Lafzäitëmfeld fir Container oder Mikroprozessoren, déi géint Manipulatioune geschützt sinn. Do ass eng extern Kontroll duerch en Drëtten ëmmer virgeschriwwen. Ouni Ausnam. – Dat ass streng. Mee am Gesetz war dach nach vun enger Kategorie fir kritesch Produite rieds. Wat ass dann do dran, wa Firewalls schonn an der Klass 2 sinn?

16:31 Dat sinn esouzesoe wierklech d’Nervezentere vun eiser ganzer Infrastruktur. – Hues de e Beispill? – Denk u Smart-Meter-Gateways, iwwer déi d’Stroumnetzer gesteiert ginn. Oder Hardware-Sécherheetsmodullen, déi kryptografesch Schlëssele fir grouss Banke verwalten. Hei geet d’EU nach méi wäit. D’Europäesch Kommissioun ka mat delegéierte Rechtsakten esouguer virschreiwen, datt fir dës Produiten en europäeschen Cybersécherheetszertifikat muss virleien. – Ier se iwwerhaapt dierfe verkaf ginn? – Genee, a mindestens op der Stuf „mëttel“ oder „héich“. Virdrun dierfe se guer net op de Marché. – Dat wäert de Marché richteg ëmkrämpelen. Da kucken ech am Geschäft net méi just no de Megapixele vun der Kamera, mee och no der Zertifizéierung a wéi laang et laut der Verpakung Updates gëtt. – Ganz genee.

Meldepflichten an Informatiounsaustausch

17:14 Mee beim Liesen ass mer nach eppes opgedaucht, wat ech wierklech kritesch gesinn. – Da schéiss lass. – Wat geschitt am Krisefall? Och mat SBOMen an onofhängege Kontrollstellen gëtt et nach ëmmer Hackerugréffer. D’Hacker sinn erfindungsräich. – Kloer. Et gëtt keng honnertprozenteg Sécherheet. – Genee. An do hunn ech am Text eppes vu Meldefriste gelies: 24 Stonnen. – Jo, d’24-Stonne-Reegel. – Stell der dat vir. A menger Firma gëtt eng Sécherheetslück aktiv ausgenotzt, bei mir brenne spréchwiertlech d’Serveren. Am IT-Service ass Panik. Mir probéieren an aller Hast, Systemer vum Netz ze huelen.

17:53 A genee an deem Moment verlaangt d’EU vu mir, datt ech mech u mäi Schreifdësch setzen a bannent 24 Stonnen iergendwellech Formulairen ausfëllen? – Genee bei där Virstellung hu vill Leit an den Direktioune bal keng Loft méi kritt. – Zu Recht! – Mee kucke mer eis emol den Oflaf méi genee un. Bei enger Sécherheetslück, déi aktiv ausgenotzt gëtt, oder bei engem schwéiere Sécherheetsvirfall muss de eng sougenannt Fréiwarnung ofginn. An dat ouni Verspéidung, spéitstens no 24 Stonnen. – U wien iwwerhaapt? – Iwwer eng zentral, eenheetlech Meldeplattform vun ENISA, der EU-Agence fir Cybersécherheet. Déi leet d’Meldung un den zoustännegen nationale Computer Security Incident Response Team weider, also un de CSIRT vun dengem Land.

18:36 Dat ass dach verréckt! Denk dat emol bis zum Schluss duerch. Ech mellen enger EU-Datebank eng grouss Sécherheetslück, fir déi et nach kee Patch gëtt. A wat, wann déi Datebank gehackt gëtt oder een, deen do schafft, sech verplappert? Dann hunn ech just eng detailléiert Uleedung geliwwert, wéi een a mäi System erakënnt. An ech hunn zu deem Zäitpunkt mol nach kee Patch fäerdeg. Dat mécht de Problem dach vill méi schlëmm. – Ech verstinn dech ganz gutt. Dat ass eng berechtegt Suerg.

19:03 Mee och doriwwer huet d'EU sech Gedanke gemaach. Et geet net drëm, Sécherheetslücken direkt an der ganzer Welt erauszeposaunen. Fir d'Weiderginn vun Informatioune gesäit d'Gesetz ganz streng Reegelen vir. – Wéi gesinn déi aus? – Aus Grënn vun der Cybersécherheet kann d'Weiderleede vun denger Meldung verréckelt ginn, oder d'Meldung ka souguer komplett anonymiséiert ginn. – Dat heescht, si halen dat geheim? – Genee. Den zoustännege CSIRT ka soen: „Wa mer dat elo un aner Staate weiderginn, riskéiere mer eng Katastroph. Mir behalen d'Informatioun ënner Verschloss, bis den Hiersteller de Patch ausgeliwwert huet." – Ah, okay. – An als Hiersteller muss de spéitstens 14 Deeg, nodeems dës Korrektur zur Verfügung gestallt gouf, en detailléierten Ofschlossrapport noreechen. Virdru bleift dat dacks staark ofgeschiermt.

19:45 Si setzen d'Informatiounen also gewëssermoossen a Quarantän. Mee firwat dann déi immens Hetz? Firwat soll ech mech an deenen éischte 24 Stonnen esou ploen, wann d'Meldung duerno souwisou fir d'éischt ënner Verschloss bleift? – Wéinst dem europäesche Bannemaart an deem, wat een „blast radius" nennt. – „Blast radius", also wéi wäit de Schued reeche kann? – Genee, bei engem Hackerugréff. E Server, dee bei engem Hiersteller a Frankräich brennt, ass haut fir hie vläicht just e lokale Problem. Muer de Moien ass dat awer e Sécherheetsproblem fir e ganze System, fir vernetzte Spideeler an Däitschland a Stroumnetzer an Italien.

20:20 Jo, dat liicht mer an. Duerch déi Fréiwarnung bannent 24 Stonne wëssen déi national Ofwierzentren direkt: „Opgepasst, do kënnt eng Well op eis zou." Si kënne kritesch Infrastrukture warnen, bestëmmten Dateverkéier blockéieren an Netzwierker ofschiermen, ier sech den Ugréff iwwerall ausbreet. Dat ergëtt wierklech Sënn, dat muss ech zouginn. E bësse wéi e Fréiwarnsystem fir Tsunamien. – Genee dat ass et. – Mee wat geschitt, wann eng Entreprise sech einfach net un déi 24 Stonnen hält? Oder wann se fuddelt a guer kee sécheren Design virgesäit? Bei wat fir Sanktioune si mer do? D'Konsequenz ass wuel méi wéi e béise Bréif vu Bréissel?

Maartiwwerwaachung an Datumer vun der Uwendung

20:55 An ob. D'Maartiwwerwaachungsautoritéite kréie wierklech Mëttelen an de Grapp. Si kënnen e Produit a ganz Europa zeréckruffe loossen. Dat schuet dem Ruff vun der Firma a kascht se enorm vill Suen. – A Geldstrofen? – Jo, si kënne ganz héich Geldstrofe verhänken, Zommen am zweestellege Milliouneberäich oder e Prozentsaz vum weltwäite Joresëmsaz. Et zielt dee Montant, dee méi héich ass. – Dat deet wéi.

21:23 Mee fir op d'Verhältnisméissegkeet zeréckzekommen: Et gëtt Ausnamen, fir datt Startuppen a ganz kleng Betriber net wéinst engem reng formelle Feeler direkt ënnerginn. – E Gléck. – Mikroentreprisen a kleng Betriber kréie keng Geldstrof, wa se just déi extrem kuerz Frist vu 24 Stonne verpassen, virausgesat, datt se soss kooperativ

mat den Autoritéiten zesummeschaffen. – E bësse Gnod fir déi Kleng. Dat ass fair. Wéi vill Zäit huet d’Industrie iwwerhaapt nach, fir sech vun hiren ale Gewunnechten ze trennen? Wéini hëlt de Sheriff an dësem digitale Wëlle Westen den Déngscht op?

21:58 De Kalenner ass stramm, mee d’Reegele gëllen a méi Etappen. De CRA gëllt am Allgemengen ab dem 11. Dezember 2027. Dat ass deen Dag, vun deem un déi nei CE-Markéierung an d’Flichte fir den Design definitiv gräifen. Mee opgepasst: D’Flicht, Sécherheetslücken a Virfäll ze mellen, also déi 24-Stonne-Reegel, iwwer déi mer elo am Detail geschwat hunn, gräift scho méi wéi ee Joer éischter, nämlech den 11. September 2026. Vun deem Datum un tickt am Krisefall d’Auer.

22:28 Onheemlech. Looss eis dat kuerz zesummefaassen, dat war ganz vill op eemol. Fir de Wëlle Weste vun den onsécheren IoT-Geräter an all där Software voller Lächer gëtt et endlech streng Reegelen. Vun der einfacher Smart-Home-Kamera iwwer de Passwuertmanager bis an de Mikroprozessor eran ass Sécherheet an Zukunft schonn ab Wierk gesetzlech virgeschriwwen. – Richteg. Fënnef Joer garantéiert Updates ginn zur Norm. Mat enger SBOM mussen d’Hiersteller genee wëssen, wéi eng digital Zoutaten an hire Produite stiechen. Wie mat Open Source Sue verdéngt, haft dofir. A bei engem Hackerugrëff muss een dat bannent 24 Stonnen iwwer e ganz séchere System mellen. – Dat resuméiert et präzis.

23:09 Et ass wierklech e risege Schrëtt. Wie weider op deem lukrativen EU-Marché verkafe wëll, muss sech upassen, egal ob d’Firma zu München, am Silicon Valley oder zu Shenzhen sëtzt. An dat ass mäi wichtegste Rot fir dech, wann s de eis grad nolauschters: Wann s de an Zukunft Software fir doheem keefs oder am Büro eng nei IT-Léisung aféiers, da fro de Verkeefer selwer no der SBOM. Fro och ganz genee, bis wéini de Support garantéiert ass. – E ganz gudden Tipp. Vum Zäitpunkt un, wou de CRA gëllt, hues de e gesetzlecht Recht op déi Äntwerten. Du keefs dann am digitalen Ëmfeld keng Kaz méi am Sak. – Absolutt. Du keefs e Produit, fir deen den Hiersteller ëmfaassend Rechenschaft ofleeë muss.

Produkthaftung an Ofschloss

23:54 Haut hu mer vill iwwer Geldstrofen a Verstéiss geschwat. Wéi ech den Text nach emol gelies hunn, ass mer nach eppes opgefall. – Wat dann? – Dat ass mer virdru bal laanscht d’Nues gaangen, mee et huet et a sech. Am Erwäägungsgrond 31 steet e ganz klengen, onopfällege Querverweis. – Ech menge schonn ze wëssen, wou s de hiwëlls. – Do steet, datt de Cyber Resilience Act an déi nei EU-Richtlinn iwwer d’Produkthaftung Hand an Hand ginn. D’Reglement 2024/2853. – O jo, d’Richtlinn iwwer d’Produkthaftung.

24:30 Dat ass déi juristesch Ofrësskugel, déi deem Ganzen eng aner Dimensioun gëtt. Looss der dat emol duerch de Kapp goen: Dës Richtlinn féiert fir Software de Grondsaz vun der verscholdensonofhängeger Haftung an. Dat ass eppes Grousses. Konkret heescht dat: En Hiersteller liwwert dir e Sécherheetsupdate net mat Zäiten, obwuel en nom CRA verdammt nach emol dozou verflicht ass. Doduerch entsteet dir als Benotzer e Schued. Zum Beispill gëtt däi Firmennetz duerch genee déi Lück lamgeluecht, oder

deng Kontodonnéeë ginn iwwer de Babyphone geklaut. Da kéints de direkt géint den Hiersteller op Schuedenersaz kloen.

25:05 Richteg. Onofhängeg dovun, ob den Hiersteller den Hackerugréff direkt verursaacht huet. Eleng den Update, dee feelt, geet fir d’Haftung duer. Hei geet et also net méi nëmmen ëm Geldstrofen, déi un de Staat bezuelt ginn, mee ëm zivilrechtlech Kloe vu Benotzer, bei deenen et ëm Milliounе geet. – Elo geet mer e Liicht op: Kéint d’Angscht virun esou risege Schuedenersazfuerderungen der Techbranche endlech deen ale Motto aus dem Silicon Valley ausdreiwen: „Move fast and break things“?

25:31 Dat ass eng ganz gutt Schlussfolgerung. Genau dorop leeft et eraus. „Move fast and break things“ funktionéiert just esou laang, wéi een net fir dat bezuele muss, wat futtigeet. An dat ännert sech elo fir ëmmer. – Ech géif soen, fir d’Software fänkt eng ganz nei Zäit un. Denk mol drun, wann s de haut den Owend deen nächsten Update op dengem Handy installéiers. Bis elo war Cybersécherheet dacks eng Fro vu Glawen. Mat dem Cyber Resilience Act gëtt elo endlech probéiert, Sécherheet siichtbar a moossbar ze maachen a virun allem d’Méiglechkeet ze schafen, se viru Geriicht anzefuerderen. Dat war eisen Abléck an d’Thema vun haut. Bleift virwëtzeg!