Cyber Resilience Act – Transcription du podcast

Audio en allemand · transcription en français · 26:05

Traduction française de l’entretien en allemand, révisée pour la lecture et accompagnée de repères temporels. Les précisions éditoriales éclairent certaines formulations de l’enregistrement.

Précisions sur les points abordés

Précisions éditoriales à jour au 15 novembre 2026.

Assistance et mises à jour. La période d’assistance est en principe d’au moins cinq ans. Si le produit est censé être utilisé moins longtemps, elle peut correspondre à cette durée. Les mises à jour de sécurité automatiques sont prévues lorsque cela est applicable.

Nomenclature logicielle. La SBOM doit couvrir au minimum les dépendances de premier niveau. Cette obligation documentaire ne donne pas à tout acheteur un droit général à la communication de la SBOM complète.

Notifications. L’article 14 s’applique depuis le 11 septembre 2026. En cas de vulnérabilité activement exploitée ou d’incident de sécurité grave, le fabricant transmet en principe une alerte précoce dans les 24 heures après en avoir pris connaissance, puis une notification dans les 72 heures. Le délai du rapport final dépend du cas.

Responsabilité du fait des produits. Le texte (UE) 2024/2853 est une directive. L’absence de mise à jour peut contribuer à établir la défectuosité. Il faut également un dommage indemnisable et un lien de causalité. Les dommages aux biens et aux données à usage exclusivement professionnel sont exclus du champ de cette directive.

Marquage CE. Selon l’article 30, paragraphe 4, du CRA, le numéro de l’organisme notifié suit le marquage CE lorsque cet organisme intervient dans la procédure d’assurance complète de la qualité prévue par le module H.

(EU) 2024/2847 · (EU) 2024/2853 · Notifications au titre du CRA

Le babyphone connecté et le champ d’application

00:00 Imagine que tu achètes une voiture toute neuve. – Oui, d’accord. – Une belle voiture neuve. – Exactement. – Tu quittes le concessionnaire, tu accélères sur l’autoroute jusqu’à 130 km/h et, là, tu t’aperçois que le constructeur a tout simplement oublié les freins. – Ce serait plutôt ennuyeux, oui. – Carrément. Paniqué, tu appelles le service clientèle, et on te répond tranquillement : « Ah, désolé, les plaquettes de frein, c’est à vous de les télécharger sur Internet et de vous débrouiller pour les monter. Bonne chance ! » – C’est complètement absurde. – Oui. – Tout le monde porterait plainte. – Évidemment.

00:34 Pourtant, dans le numérique, on achète tous les jours des serrures connectées, des babyphones ou des routeurs Wi-Fi pour lesquels c'est exactement ce qui se passe. – Hélas, oui. – On achète un produit inachevé. – Voilà. Un produit inachevé et vulnérable, et c'est l'acheteur qui assume tout le risque. Du moins jusqu'à aujourd'hui. L'Union européenne vient d'appuyer sur le bouton d'arrêt d'urgence, avec une force difficile à imaginer. Toute l'industrie technologique mondiale va en ressentir la secousse. – Bien dit.

01:06 Bienvenue dans notre analyse du jour. Merci d'être à nouveau là, en quelque sorte notre troisième interlocuteur dans la pièce. – Merci de nous écouter. – Aujourd'hui, on s'intéresse à un sujet qui, à première vue, a tout de la bureaucratie bruxelloise la plus aride. – Mais ce n'est pas le cas ? – Pas du tout. C'est en réalité un séisme réglementaire. On parle du nouveau règlement européen 2024/2847, plus connu sous le nom de « Cyber Resilience Act », ou CRA. – Exactement. Notre seule source aujourd'hui est le texte juridique officiel de l'UE. Pas de panique, on va le traduire en termes de tous les jours. Voyons ensemble de quoi il s'agit.

01:47 Entrons dans le vif du sujet. Pour rendre les choses concrètes, j'ai pensé qu'on pourrait inventer un produit et lui appliquer les règles. Appelons-le le Smart Baby 3000. – Le Smart Baby 3000, ça me plaît. Que fait-il ? – C'est un babyphone dernier cri connecté au Wi-Fi, avec caméra HD, application pour smartphone reliée au cloud, tout y est. – Qu'est-ce que le CRA va changer dans la vie de cet appareil en particulier ? – Pour le comprendre, il faut commencer par le champ d'application de ce nouveau règlement.

02:19 Le CRA vise tous les « produits comportant des éléments numériques » ; je cite le texte. – Ça paraît extrêmement large. – Ça l'est. Il s'agit de produits dont l'usage prévu comprend une connexion de données, directe ou indirecte, logique ou physique, à un appareil ou à un réseau. – Donc notre Smart Baby 3000 entre en plein dedans. – Absolument, puisqu'il combine matériel et logiciel et que son fonctionnement repose sur une connexion. Les exceptions concernent essentiellement des domaines déjà encadrés par une législation sectorielle très stricte. – Comme les dispositifs médicaux ou les avions ? – Exactement. L'automobile, l'aviation, le secteur médical connaissent déjà des exigences sévères.

02:57 Attends. Le babyphone lui-même est bien là, dans la chambre de mon enfant. Mais qu'en est-il de l'application et du cloud ? – Très bonne question. – Le signal vidéo transite souvent par un serveur installé à l'étranger. L'UE réglemente-t-elle uniquement le boîtier en plastique et la puce, ou ce cloud est-il lui aussi concerné ?

03:17 Cette distinction est importante. En principe, le CRA réglemente des produits et non les services fournis isolément. Mais, et la nuance est de taille, le traitement de données à distance, ici dans le cloud, relève du CRA lorsque le produit ne pourrait pas remplir sa fonction sans lui. – D'accord. – Si ton Smart Baby 3000 ne peut afficher aucune image sur ton téléphone sans l'interface du serveur du fabricant, ce composant cloud fait juridiquement partie du produit réglementé. – Ah oui ! Le fabricant ne peut donc pas dire : « Notre appareil est sûr, c'est juste le serveur, là-bas, qui a malheureusement été piraté. » – Exactement. Cet argument ne tient plus. Il répond de l'ensemble.

Réglages de sécurité et responsabilités dans la chaîne de distribution

03:54 Je comprends. Mais qu’exige l’UE concrètement ? Le fabricant peut-il mettre son appareil sur le marché et fournir un correctif plus tard, par exemple après que des pirates ont parlé dans la chambre de l’enfant avec des voix effrayantes ? – Plus maintenant. Cette époque est révolue. Au cœur du règlement, il y a le principe de sécurité dès la conception et par défaut. – Donc, dès la sortie d’usine. – Tout à fait. Jusqu’ici, on pensait souvent à la sécurité après coup, comme un pansement sur une plaie ouverte. – Avec l’idée qu’on enverrait bien un correctif plus tard. – Voilà. Le législateur oblige désormais les fabricants à mettre sur le marché des produits exempts de vulnérabilités exploitables connues. Cette obligation commence dès la planche à dessin. – Impressionnant.

04:33 Cela inclut la minimisation des données. Le babyphone ne doit pas collecter en secret des métadonnées à des fins publicitaires si elles ne sont pas nécessaires à son fonctionnement. – Voilà qui est rassurant pour un babyphone. – N’est-ce pas ? Et surtout, la protection contre les accès non autorisés doit être activée par défaut. – Les fameux mots de passe standard, « Admin123 » ou « 0000 », inscrits en dur dans des millions d’appareils, deviendraient donc illégaux ? – Tout à fait. Chaque appareil doit avoir ses propres identifiants ou t’obliger, au premier démarrage, à choisir un mot de passe vraiment sûr. – Enfin !

05:13 L’aspect économique est particulièrement intéressant. L’UE intervient pour corriger une défaillance classique du marché. – Qu’entends-tu par là ? Une asymétrie d’information ? – Exactement. L’utilisateur ordinaire n’a aucun moyen d’évaluer la sécurité d’un appareil domotique complexe. – Non, effectivement. On voit juste qu’il est joli et qu’il fonctionne. – Voilà. Impossible de voir si, derrière le boîtier, le code est troué comme du gruyère. Le fabricant, lui, le sait. Mais il n’avait jusqu’ici aucune incitation financière à investir dans cette sécurité invisible. – Bien sûr. Le design du boîtier se vend mieux que la qualité du code. – Exactement. Le CRA transfère radicalement cette charge économique vers le fabricant.

05:54 D’accord, celui qui construit le produit doit investir. Mais soyons honnêtes : un babyphone comme celui-là est généralement fabriqué quelque part en Asie. – Souvent, oui. – Ensuite, un petit importateur le fait venir en Europe, et il atterrit dans les rayons d’une grande enseigne d’électronique. Si le fabricant asiatique dit : « Vos règles européennes ne m’intéressent pas », que se passe-t-il ? Les distributeurs européens s’en tirent-ils à bon compte ? – Pas du tout. L’UE a tiré les leçons de ses réglementations précédentes. Cette fois, elle implique toute la chaîne d’approvisionnement. – Même le magasin d’électronique du coin ?

06:27 Oui. Les importateurs et les distributeurs dans l’UE partagent la responsabilité. Si une grande enseigne achète ces gadgets domotiques bon marché par conteneurs entiers à l’étranger, elle ne peut les distribuer que s’ils portent le marquage CE et si leur sécurité informatique est démontrée. – Le distributeur doit donc vérifier ? – Exactement. Dès lors qu’un distributeur a des raisons de penser que ce Smart Baby 3000 présente

un risque, il ne peut même pas le mettre en rayon. Il doit le bloquer et informer immédiatement les autorités.

Logiciels libres et activité commerciale

06:55 Là, il faut que je t'arrête. C'est très bien en théorie, mais ça ne se heurte pas à la réalité du développement logiciel ? – En quel sens ? – Aujourd'hui, presque tout produit commercial moderne contient des composants open source. Le fabricant de mon Smart Baby 3000 ne réécrit pas intégralement le système d'exploitation. – C'est vrai. – Il prend un Linux libre, y ajoute une bibliothèque open source pour la caméra récupérée sur GitHub, et voilà. Si ce code libre écrit par des bénévoles se révèle vulnérable, qui en répond ?

07:26 Je vois où tu veux en venir. – On a l'impression que cette loi risque d'étouffer toute la communauté du logiciel libre. Si, le week-end, je développe dans ma cave une extension domotique sympa et que je mets sur mon site un petit lien Patreon pour qu'on m'offre un café, risque-t-on soudain de me réclamer des millions si mon code est piraté ? Parce que, franchement, si c'est ça, je le retire dès aujourd'hui. – Respire. Tu peux laisser ton code en ligne tranquillement. – Ouf ! – Mais tu mets le doigt sur ce qui a le plus inquiété la communauté open source à la publication des premières versions du texte. – On le comprend. – Tout à fait.

08:03 Si on regarde de près les considérants 17 à 19, on voit comment le législateur a résolu la question. Le CRA distingue nettement la phase de développement de celle de la fourniture commerciale. – Concrètement, qu'est-ce que ça veut dire ? – Les logiciels libres et ouverts, ou FOSS, ne sont soumis à ces obligations strictes que s'ils sont mis à disposition dans le cadre d'une activité commerciale. – Et mon bouton Patreon pour le café ? – Ce n'est pas une activité commerciale. Les dons sans but lucratif font expressément l'objet d'une exception dans le texte. – Très bien.

08:38 Cela devient commercial quand tu monétises activement le logiciel ou quand tu proposes, par exemple, une assistance technique payante. Ou encore, et c'est là le point décisif pour les entreprises, lorsqu'une grande société récupère ce code gratuit écrit pendant les loisirs de quelqu'un et l'intègre, pour en tirer profit, à son routeur ou à son babyphone commercial. À ce moment-là, en tant que fabricant du produit final, elle répond pleinement de la sécurité de ces composants open source. – C'est bien pensé. Le fabricant du Smart Baby 3000 ne peut plus dire : « Ce n'est pas notre faute si la bibliothèque libre de la caméra avait un bug. » – Exactement. Il gagne de l'argent sur l'ensemble, il doit aussi garantir la sécurité des éléments gratuits qu'il y a intégrés. – On protège ainsi l'innovation des petits développeurs tout en responsabilisant les géants de la tech. Plutôt malin.

09:31 Mais que se passe-t-il pour les grandes fondations open source ? – Comme la fondation Apache ? – Oui. Elles produisent des logiciels qui semblent faire tourner la moitié d'Internet, tout en étant souvent des organismes sans but lucratif. – La loi crée justement un nouveau rôle, celui d'« intendant de logiciels ouverts ». – C'est assez solennel. – Ça l'est. Il s'agit de personnes morales qui soutiennent le logiciel libre de

manière systématique et durable sans vendre de produits finis comme le ferait un fabricant classique. – Pourquoi leur consacrer un statut particulier ?

10:09 Parce que l'UE a compris que si on infligeait des millions d'euros d'amende à une fondation comme Apache, Internet s'effondrerait demain. Les obligations des intendants sont donc allégées. – On les ménage un peu ? – Si on veut. Ils doivent disposer d'une politique de cybersécurité documentée et traiter les vulnérabilités de manière professionnelle. – Bien sûr. – En revanche, par exemple, ils ne sont pas autorisés à apposer le marquage CE et le texte les protège expressément contre de lourdes amendes. L'objectif n'est pas de les ruiner. – D'accord. On a donc vu la conception et toute la phase de développement.

Mises à jour, assistance et nomenclature logicielle

10:44 Passons à ce qui se passe après l'achat. – Volontiers, la phase d'utilisation. – J'utilise mon Smart Baby 3000 depuis trois ans. Un chercheur en sécurité découvre une faille majeure dans la bibliothèque de la caméra. – Le grand classique. – Jusqu'ici, la réponse du fabricant était souvent : « Ce modèle est ancien. Achète donc le nouveau Smart Baby 4000. » Que prévoit maintenant le CRA pour les mises à jour ? – C'est là que la réglementation va faire mal à beaucoup de fabricants. Elle impose une période d'assistance garantie.

11:17 Une période d'assistance ? – Oui. C'est la période pendant laquelle des mises à jour de sécurité doivent être fournies. Elle doit correspondre à la durée d'utilisation prévisible du produit et elle est en principe d'au moins cinq ans. – Cinq ans ? Une éternité dans le monde de la tech ! – Il y a des exceptions lorsque la durée de vie du produit est par nature nettement plus courte. – Une application provisoire pour un événement, par exemple. – Mais pour un appareil physique, on parle généralement d'au moins cinq ans.

11:48 Est-ce que les mises à jour doivent arriver automatiquement ou vais-je devoir fouiller sans cesse dans des menus obscurs pour cliquer sur « Rechercher des mises à jour » ? – C'est l'autre grand changement. Le législateur demande que les produits soient conçus pour que les mises à jour de sécurité soient téléchargées et installées automatiquement par défaut. – Super ! – Tu disposes bien sûr d'un moyen simple de désactiver ce mécanisme, mais le réglage par défaut reste automatique. Une autre disposition est intéressante : les mises à jour fonctionnelles doivent être séparées des mises à jour de sécurité. – Merci, l'Europe. Je ne serai donc plus obligé d'installer une nouvelle interface gourmande en mémoire pour corriger une minuscule faille. – Exactement. On dissocie la partie sécurité du reste. C'est vraiment pratique pour l'utilisateur.

12:36 C'est maintenant que commence le travail d'Hercule pour les fabricants. – Lequel ? – Comment le fabricant du Smart Baby 3000 peut-il savoir, trois ans plus tard, que cette bibliothèque open source vulnérable, vieille de trois ans, se cache au cœur de son code ? – C'est là qu'intervient ce sigle qui fait transpirer toute l'industrie informatique : la SBOM ? – Exactement, « software bill of materials », autrement dit une nomenclature logicielle. Le CRA impose aux fabricants d'établir et de tenir à jour une liste lisible par

machine de tous les composants, bibliothèques et dépendances présents dans leur produit.

13:16 Si on transpose ça à la vie de tous les jours, c'est la liste des ingrédients sur un emballage alimentaire, en somme ? – Tout à fait. – Quelqu'un d'allergique aux arachides retourne le paquet pour vérifier s'il y en a. Si on découvre une faille dans un morceau de code, le fabricant consulte sa liste d'ingrédients, sa SBOM, et voit immédiatement : « Mince, ce code vulnérable est dans notre babyphone. Il faut corriger ça tout de suite. » – Très bonne image. Imagine maintenant que la liste compte des centaines de milliers d'entrées et que certains ingrédients contiennent à leur tour des dizaines de sous-ingrédients fournis par des gens que tu ne connais même pas. – Ça ressemble à un cauchemar.

13:55 Ça en est un. Mais si on prend du recul, on comprend pourquoi la SBOM change la donne. Tu te souviens de Log4j ? – Oh oui ! – C'était une petite bibliothèque de journalisation en Java qu'on retrouvait pratiquement partout. Quand une faille y a été découverte, la panique a été mondiale. De grands groupes ont mis des semaines simplement à déterminer lesquels de leurs systèmes utilisaient Log4j. – Un effet papillon gigantesque. – Exactement. Avec des SBOM, on parcourt automatiquement les nomenclatures et on sait en une fraction de seconde quels produits sont concernés. Les reconstituer pour du code ancien est un énorme défi logistique, mais pour l'avenir, c'est indispensable.

Risques du produit, conformité et marquage CE

14:35 D'accord. Nous avons donc une conception sécurisée, cinq ans de mises à jour automatiques et une liste complète des ingrédients. Mais qui contrôle tout ça ? L'UE fait-elle simplement confiance aux fabricants ? Est-ce que quelque chose changera sur l'emballage de mon babyphone ? – Le signe visible sur l'emballage restera le marquage CE, mais sa signification change profondément. – En quoi ? – Jusqu'ici, sur beaucoup d'appareils connectés, le marquage CE renvoyait surtout à la sécurité électrique, pour éviter par exemple que l'alimentation prenne feu, ou au respect de normes radio. Désormais, il devra aussi couvrir la sécurité informatique au titre du CRA. – Qui la vérifie ?

15:17 Cela dépend de la classe de risque. Pour les produits standard à faible risque, le fabricant peut toujours évaluer et documenter lui-même la conformité par contrôle interne. – Mais mon Smart Baby 3000 filme directement la chambre de mon enfant. Ce n'est pas un risque standard, si ? – Tout à fait. Ces appareils relèvent de la catégorie des produits importants comportant des éléments numériques. Ceux-ci se répartissent entre classe I et classe II. – Qu'est-ce qui relève de la classe I ? – Par exemple des appareils domestiques connectés dotés de fonctions de sécurité, des babyphones, des jouets connectés ou encore des gestionnaires de mots de passe. Si le fabricant ne suit pas strictement les normes européennes harmonisées, un organisme d'évaluation indépendant doit intervenir.

15:59 Comment l'acheteur peut-il le voir ? – Le numéro d'identification à quatre chiffres de l'organisme figure alors juste à côté du marquage CE. – Je vois. Et la classe II ? – Elle

concerne des éléments encore plus sensibles : pare-feu, environnements d’exécution de conteneurs ou microprocesseurs résistants aux manipulations. Un contrôle externe par un tiers y est toujours obligatoire, sans exception. – Quand même ! Mais le texte parle aussi d’une catégorie de produits critiques. Qu’est-ce qui reste dans cette catégorie si les pare-feu sont déjà de classe II ?

16:31 Il s’agit des véritables centres nerveux de toute notre infrastructure. – Un exemple ? – Pense aux passerelles des compteurs intelligents qui pilotent les réseaux d’électricité ou aux modules matériels de sécurité qui gèrent les clés cryptographiques des grandes banques. Ici, l’UE va très loin. La Commission peut, par actes délégués, imposer à ces produits un certificat européen de cybersécurité. – Avant même qu’on puisse les vendre ? – Oui, avec un niveau d’assurance au moins « substantiel » ou « élevé ». Avant cela, la mise sur le marché est exclue. – Ça va bouleverser le marché. Au magasin, je regarderai donc sur l’emballage, en plus du nombre de mégapixels de la caméra, sa certification et la durée de fourniture des mises à jour. – Exactement.

Notifications et partage d’informations

17:14 J’en viens au point qui m’a vraiment fait tiquer à la lecture. – Vas-y. – Que se passe-t-il en pleine crise ? Même avec des SBOM et des évaluations indépendantes, il y aura des piratages. Les pirates sont inventifs. – Évidemment. La sécurité à cent pour cent n’existe pas. – Justement. J’ai lu quelque chose sur les délais de notification : vingt-quatre heures. – Oui, la règle des vingt-quatre heures. – Mets-toi à ma place. Une vulnérabilité activement exploitée se déclare dans mon entreprise. C’est le feu dans les serveurs. Le service informatique est en pleine panique, et nous essayons désespérément d’isoler les systèmes du réseau.

17:53 Et c’est à ce moment précis que l’UE exige que je m’assoie à mon bureau pour remplir des formulaires dans les vingt-quatre heures ? – C’est le passage qui a donné des sueurs froides à bien des dirigeants. – À juste titre. – Regardons tout de même de plus près. En présence d’une vulnérabilité activement exploitée ou d’un incident de sécurité grave, il faut présenter ce qu’on appelle une alerte précoce. Et oui, sans retard injustifié et au plus tard dans les vingt-quatre heures. – À qui ? – À la plateforme unique de notification de l’Agence de l’Union européenne pour la cybersécurité, l’ENISA. Celle-ci transmet ensuite la notification à l’équipe nationale compétente de réponse aux incidents de sécurité informatique, le CSIRT du pays concerné.

18:36 Mais c’est de la folie ! Réfléchis : je signale une faille majeure, toujours sans correctif, à une base de données européenne. Si cette base est piratée ou si quelqu’un laisse filtrer l’information, je viens de fournir un mode d’emploi détaillé pour s’introduire dans mon système. Et je n’ai même pas encore de correctif prêt à déployer. Ça risque d’aggraver considérablement le problème. – Je comprends tout à fait. C’est une crainte légitime.

19:03 L’UE y a pensé aussi. L’idée n’est pas d’annoncer immédiatement au monde entier toutes les vulnérabilités. Le législateur a prévu des règles de partage d’information très strictes. – Lesquelles ? – Pour des raisons de cybersécurité, la diffusion de ta notification peut être différée ou les informations peuvent même être

entièrement anonymisées. – Donc, on garde ça confidentiel ? – Oui. Le CSIRT compétent peut conclure : « Si nous communiquons ces informations tout de suite à d'autres États, nous risquons de provoquer une catastrophe. Gardons-les confidentielles le temps que le fabricant distribue le correctif. » – Je vois. – Et le fabricant remet ensuite un rapport final détaillé au plus tard quatorze jours après la mise à disposition de la correction. D'ici là, l'information reste souvent très protégée.

19:45 Ils instaurent donc une sorte de quarantaine pour l'information. Mais franchement, pourquoi une telle urgence ? Pourquoi me mettre cette pression dans les premières vingt-quatre heures, si l'information reste d'abord confidentielle ? – À cause du marché unique européen et de ce qu'on appelle le « blast radius ». – Le rayon d'impact ? – Oui, l'étendue des dégâts d'un piratage. Un serveur en feu chez un fabricant français peut n'être, aujourd'hui, qu'un problème local pour l'entreprise. Demain matin, cela pourrait devenir un problème de sécurité systémique pour des hôpitaux connectés en Allemagne ou des réseaux électriques en Italie.

20:20 D'accord. Grâce à l'alerte précoce dans les vingt-quatre heures, les centres nationaux de défense savent immédiatement qu'une vague arrive. Ils peuvent prévenir les infrastructures critiques, bloquer certains flux et sécuriser les réseaux avant que l'attaque se propage à grande échelle. – Vu comme ça, je dois reconnaître que c'est logique. Cela ressemble aux systèmes d'alerte précoce pour les tsunamis. – C'est exactement ça. – Mais si une entreprise ignore purement et simplement ces vingt-quatre heures, ou triche plus largement en négligeant la sécurité dès la conception, quelles sont les sanctions ? Sans doute un peu plus qu'une lettre de réprimande de Bruxelles ?

Surveillance du marché et calendrier

20:55 Bien plus. Les autorités de surveillance du marché disposent de moyens d'action importants. Elles peuvent faire rappeler des produits dans toute l'Europe, avec un coût considérable pour l'entreprise et de lourdes répercussions sur son image. – Et les amendes ? – Elles peuvent être sévères. Il peut s'agir de dizaines de millions d'euros ou d'un pourcentage du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. – Ça fait mal.

21:23 Mais, pour en revenir à la proportionnalité, il existe des exceptions pour qu'une seule erreur de forme ne condamne pas immédiatement une jeune pousse ou une toute petite entreprise. – Heureusement. – Les microentreprises et les petites entreprises ne se voient pas infliger d'amende si leur seul manquement consiste à dépasser ce délai très court de vingt-quatre heures, à condition de coopérer par ailleurs avec les autorités. – Un peu de clémence pour les plus petits. C'est juste. De combien de temps l'industrie dispose-t-elle maintenant pour changer ses habitudes ? Quand ce shérif du Far West numérique entre-t-il en action ?

21:58 Le calendrier est serré, mais l'application est échelonnée. Le CRA s'applique de manière générale à partir du 11 décembre 2027. C'est à cette date que le nouveau marquage CE et les obligations de conception prennent pleinement effet. Mais attention : les obligations de notification des vulnérabilités et des incidents, dont cette fameuse

alerte de vingt-quatre heures, entrent en application plus d’un an plus tôt, dès le 11 septembre 2026. À compter de cette date, le compte à rebours commence dès qu’une crise survient.

22:28 Eh bien ! Récapitulons, car on a couvert beaucoup de choses. Le Far West des objets connectés peu sûrs et des logiciels truffés de failles se dote enfin de règles strictes. De la petite caméra domotique au gestionnaire de mots de passe, et jusque dans les microprocesseurs, la sécurité dès la sortie d’usine devient une exigence légale. – Exactement. Cinq ans de mises à jour garanties deviennent la norme. Les fabricants doivent savoir, grâce à une SBOM, quels ingrédients numériques contiennent leurs produits. Celui qui utilise commercialement un logiciel open source en répond. Et celui qui se fait pirater doit le déclarer dans un système hautement sécurisé sous vingt-quatre heures. – C’est bien résumé.

23:09 C’est un pas de géant. Les entreprises qui voudront vendre sur ce marché européen lucratif devront s’adapter, qu’elles se trouvent à Munich, dans la Silicon Valley ou à Shenzhen. Et voici mon principal conseil si tu nous écoutes : la prochaine fois que tu achèteras un logiciel pour chez toi ou que tu déploieras une nouvelle solution informatique au bureau, pose la question de la SBOM au vendeur. Demande-lui précisément à quelle date s’achève l’assistance garantie. – Très bon conseil. À compter de l’application du CRA, tu auras légalement le droit d’obtenir ces réponses. Tu n’achèteras plus un produit numérique les yeux fermés. – Exactement. Tu achèteras un produit dont le fabricant devra pleinement rendre compte.

Responsabilité du fait des produits et conclusion

23:54 On a beaucoup parlé des amendes et des manquements aujourd’hui. En relisant le texte, j’ai remarqué autre chose. – Quoi donc ? – Cela m’avait presque échappé, et c’est peut-être le point le plus marquant. Au considérant 31, il y a un renvoi très discret, presque anodin. – Je crois voir où tu veux en venir. – Il dit que le Cyber Resilience Act et la nouvelle directive européenne sur la responsabilité du fait des produits fonctionnent de concert. Le règlement 2024/2853. – Ah oui, la directive sur la responsabilité du fait des produits défectueux.

24:30 C’est le coup de massue juridique qui fait changer l’ensemble de dimension. Prends le temps d’y réfléchir : cette directive introduit pour les logiciels le principe de responsabilité sans faute. – C’est énorme. – Supposons qu’un fabricant tarde à te livrer une mise à jour de sécurité alors que, selon le CRA, c’est bel et bien son obligation légale, et que tu en subisses un dommage. Le réseau de ton entreprise est paralysé précisément par cette faille ou des données de ton compte sont volées depuis le babyphone. Tu pourrais poursuivre directement le fabricant pour obtenir réparation.

25:05 Exactement, que le fabricant ait directement causé le piratage ou non. La seule absence de mise à jour suffit à engager sa responsabilité. On parle désormais aussi de recours civils engagés par des utilisateurs pour des millions d’euros de dommages-intérêts, en plus des amendes versées à l’État. – Je viens de penser à quelque chose. Est-ce que la seule crainte de devoir payer de tels dommages-intérêts

finira par faire perdre au secteur technologique sa vieille devise de la Silicon Valley, « Move fast and break things », aller vite quitte à casser des choses ?

25:31 C’est une excellente conclusion, parce que c’est précisément ce qui découle de tout cela. « Move fast and break things » fonctionne seulement tant qu’on ne doit pas payer pour ce qui casse. Et ça, ça va changer pour de bon. – Une nouvelle ère pour le logiciel, je dirais. Penses-y ce soir quand tu installeras la prochaine mise à jour sur ton téléphone. Jusqu’ici, la cybersécurité relevait souvent de l’acte de foi. Avec le Cyber Resilience Act, on tente enfin de rendre la sécurité visible, mesurable et surtout susceptible d’être exigée devant un tribunal. Voilà pour notre analyse du jour. Restez curieux !