C3A, ou la défiance méthodique / C3A, oder das methodische Misstrauen

□□ Fin avril 2026. Le BSI (Bundesamt für Sicherheit in der Informationstechnik / Office fédéral de la sécurité des technologies de l’information) publie un document de quelques dizaines de pages, en téléchargement libre sur son site. Titre sobre : *Criteria enabling Cloud Computing Autonomy*. Pas de communiqué tonitruant, pas de conférence de presse. Juste un PDF, déposé sur le serveur, signé Bundesamt für Sicherheit in der Informationstechnik.

À première vue, c’est un document technique de plus dans la longue tradition allemande des référentiels de cybersécurité. C5, IT-Grundschutz, BSI-Standards. Le BSI a l’habitude. Mais quand on lit C3A en détail, quelque chose ne colle pas avec le ton habituel.

Les critères ne sont pas génériques. Ils sont trop précis.

90 jours déconnecté. Sauvegarde du code source toutes les 24 heures, cinq versions minimum. Des ingénieurs locaux capables de compiler et de livrer un correctif d’urgence sans dépendance tierce. Un format portable du code, de la documentation et des outils d’administration, exploitable par l’administration fédérale. Une clause d’état de défense permettant à l’État de reprendre physiquement la plateforme.

Lu d’une traite, on aurait le réflexe d’en sourire et de parler de paranoïa. Le mot tombe vite, et il est commode. Mais il est faux. Ce que C3A met en scène, ce n’est pas une pathologie. C’est une défiance méthodique : la décision froide, assumée, documentée, de ne pas faire reposer la

continuité d’un État sur la bonne volonté d’un fournisseur, d’une juridiction étrangère ou d’un marché. La défiance, ici, n’est pas une humeur. C’est une discipline. Et cette discipline, on va le voir, dépasse largement le seul sujet du cloud.

Un référentiel de conformité ne se rédige pas dans le vide. Chaque critère est la cristallisation d’une crainte, d’un retour d’expérience, d’un war game qu’on a fait tourner en salle fermée et dont on a tiré des conclusions. Les chiffres précis (90 jours, 24 heures, 5 versions) ne sont pas des incantations. Ce sont des paramètres. Quelqu’un, quelque part dans les bureaux de Bonn, a modélisé un scénario, mesuré combien de temps il fallait tenir, et combien de redondance il fallait pour le faire.

Alors essayons de remonter le fil. Quel scénario justifie ce niveau de précision ?

Le mardi matin

Imaginons.

Mardi matin, un peu avant huit heures, heure d’Europe centrale. Quelque part hors de l’Union européenne (la géographie importe peu, l’asymétrie suffit), une décision politique tombe. Elle ne fait pas la une immédiatement. Elle prend la forme d’un ordre administratif, d’une décision d’agence, d’un courrier signé par un sous-secrétaire d’État. Le contenu est sec : un fournisseur cloud établi sous cette juridiction reçoit instruction de cesser, en tout ou partie, de servir un État européen précis. La raison invoquée (sanctions, sécurité nationale, contrôle à l’exportation) ne change rien à la mécanique. L’ordre est légal dans le pays d’origine du fournisseur. Le fournisseur doit obéir.

À 8h17, les premières alertes remontent dans les ministères concernés à Berlin. Une console d’administration cesse de répondre. Un service d’authentification fédéré refuse de

nouvelles sessions. Un cluster bascule en mode lecture seule sans qu'aucune raison technique ne l'explique. Les équipes opérationnelles ouvrent un ticket. Le ticket reste sans réponse.

À 9h12, un appel arrive depuis la filiale européenne du fournisseur. La voix au bout du fil est embarrassée. Les équipes du siège ont reçu instruction de couper le contact. Les ingénieurs européens (formellement employés par une entité européenne, payés en euros, vivant à Munich, Dublin, Paris) n'ont jamais eu les droits de commit sur le code de production. Ils n'ont jamais détenu les clés de signature. Le control plane qu'ils opèrent au quotidien est piloté depuis Seattle ou Redmond. Et ce matin, Seattle ou Redmond ne répond plus.

À 10h30, la réunion de crise commence. Autour de la table, des fonctionnaires du BMI, du BSI, des opérateurs ministériels, des juristes. Ils découvrent, ou redécouvrent, trois choses. Premièrement, le control plane est hors de portée et le restera tant que l'ordre politique ne sera pas levé. Deuxièmement, les binaires qui tournent localement continuent à fonctionner pour l'instant, mais la prochaine validation de licence cloud est programmée dans 72 heures, et personne ne peut prédire ce qui se passera ensuite : dégradation silencieuse, basculement en mode démo, arrêt pur et simple. Troisièmement, si une vulnérabilité critique est divulguée cette semaine (un zero-day sur un composant largement déployé), il n'y a, sur le sol européen, personne pour produire et livrer le correctif. Les pipelines de build sont chez le fournisseur. Les signataires aussi.

L'après-midi, on entre dans la phase de cartographie des dégâts. La paie des fonctionnaires du Land de Bavière passe par un service hébergé chez ce fournisseur. Le système d'admission de plusieurs hôpitaux universitaires aussi. Une partie de la logistique de la Bundeswehr (non classifiée, mais critique pour le quotidien) également. Le système

d’information fiscale, partiellement. Le portail citoyen pour le renouvellement des passeports. L’application qui gère les contrôles aux frontières terrestres. La plateforme d’échange entre l’administration fédérale et les Länder.

Mercredi, les médias parlent de tensions diplomatiques. À huis clos, on parle d’autre chose. On parle de continuité de l’État. On parle des fonctionnaires qui doivent être payés vendredi. Des patients qui doivent être admis ce soir. Des passeports qui doivent être renouvelés cette semaine. Des choses qui n’attendent pas la résolution diplomatique d’une crise qui peut durer des semaines, des mois, ou ne jamais se résoudre dans sa forme initiale.

Jeudi, la question opérationnelle est posée à voix haute pour la première fois. Pas « comment récupérer l’accès au service ». Mais « comment faire tourner ce service sans eux ». Et au-delà : « si la situation s’aggrave et que l’état de défense est déclaré, sommes-nous capables d’entrer dans les data centers de Francfort et de Berlin, de prendre les clés, et de faire fonctionner cette plateforme nous-mêmes (avec nos ingénieurs, nos outils, notre code) pendant le temps qu’il faudra ? »

À ce moment précis, on découvre que la réponse dépend entièrement de ce qui a été préparé avant.

Et c’est là que C3A entre en scène.

Le même mardi, mais après C3A

Rejouons la séquence. Même mardi. Même ordre tombé d’ailleurs. Même filiale européenne réduite au silence. Mais cette fois, l’État client, et le fournisseur qui le sert, ont passé les deux dernières années à se conformer à C3A.

À 8h17, les premières alertes remontent. Mais elles remontent dans un environnement où le SOC est en Allemagne, opéré par des ingénieurs allemands, qui n’ont reçu aucune consigne de

Seattle parce qu'ils ne dépendent pas de Seattle. La déconnexion observée est interprétée pour ce qu'elle est : un signal extérieur, pas une panne interne. La cellule de crise est convoquée à 8h30 : pas pour comprendre ce qui se passe, mais pour décider à quelle vitesse activer un plan qui existe.

À 9h00, la décision est prise : on déclenche le mode déconnecté. Pas dans la panique, mais selon une procédure documentée, testée annuellement comme l'exige SOV-4-09. Toutes les connexions réseau vers des entités non-UE sont coupées de manière contrôlée. Les heartbeats, les serveurs de validation de licences, les canaux de mise à jour, les flux de télémétrie. Plus rien ne sort, plus rien n'entre. La plateforme se referme sur elle-même, et continue de fonctionner.

Elle peut continuer parce que le code source qui la fait tourner est sauvegardé dans l'UE, datant de moins de 24 heures, en cinq versions au moins, dans un format que les ingénieurs locaux savent compiler. Parce que ces ingénieurs existent (SOV-6-02-AC l'exige) : du personnel spécialisé, sur le sol européen, avec des environnements de build locaux capables de produire des correctifs de sécurité d'urgence sans aucune dépendance externe. Parce que les clés de chiffrement des données sensibles n'ont jamais été dans l'environnement du fournisseur : SOV-3-02 et SOV-3-05 l'imposaient. Le fournisseur ne pouvait pas les livrer même s'il était contraint de le faire. Elles sont restées chez le client, dans son propre HSM, sur son propre sol.

À 10h30, la réunion de crise commence. Mais ce n'est plus une cellule de crise au sens dramatique. C'est une revue de situation. Le SOC confirme : les services tournent. La paie de vendredi est sécurisée. Les hôpitaux admettent normalement. Les passeports continuent de s'imprimer. Le mode déconnecté est conçu pour tenir 90 jours, l'horizon retenu par SOV-4-10. Quatre-vingt-dix jours, c'est le temps qu'il faut pour qu'une crise politique se résolve, ou pour qu'on stabilise une

alternative.

Mercredi, on commence à patcher. Une CVE est publiée sur un composant largement déployé. Dans le scénario sans C3A, c'était la catastrophe. Ici, les ingénieurs allemands récupèrent le correctif depuis les sources, le compilent dans leur environnement de build local, le signent avec leurs propres certificats, le déploient via leur pipeline souverain. Cela prend trente-six heures au lieu de douze, parce qu'on n'a pas l'habitude de le faire seuls. Mais cela se fait.

Jeudi, la question stratégique se pose dans des termes radicalement différents. Pas « combien de temps tiendrons-nous ». Mais « combien de temps est-il acceptable de tenir avant de prendre des décisions structurelles ». La capacité de reprise existe. SOV-2-03 prévoit qu'en cas d'état de défense, l'administration fédérale peut prendre la main sur les actifs physiques, le personnel, le code source, les outils d'administration (en format portable, c'est-à-dire dans une forme qu'un autre opérateur peut effectivement faire tourner). Le kit de reprise a été préparé. Il dort dans un coffre. Il peut être ouvert.

L'ordre tombé mardi matin n'a pas disparu. La crise diplomatique est toujours là. Mais elle ne dicte plus le rythme des hôpitaux, des paies, des frontières. L'asymétrie initiale (vous dépendez de nous, nous ne dépendons pas de vous) a été désarmée par deux ans de préparation méthodique.

Une doctrine, pas une obsession

Quand on relit C3A après cet exercice, le document change de nature. Ce n'est plus un référentiel de conformité abstrait. C'est l'inventaire ordonné d'une doctrine de continuité étatique face à un risque de coercition extraterritoriale par voie technologique.

Les Allemands ne disent pas que ce mardi arrivera. Ils ne le prédisent pas. Ils ne le souhaitent pas. Ils constatent

simplement que les conditions de possibilité de ce mardi existent (dans la concentration du marché cloud, dans l'extraterritorialité de certaines législations, dans le couplage profond entre les opérations européennes et les sièges hors UE), et ils en tirent les conséquences. Pragmatiques. Méticuleuses. Ordonnées.

C3A n'est pas un document optimiste. C'est un document qui suppose que la bonne volonté des juridictions étrangères n'est pas une stratégie. Que la souveraineté n'est pas un slogan, mais une suite d'exigences techniques précises qu'on peut tester un par un. Et que la continuité de l'État ne peut pas, structurellement, dépendre d'une boucle de validation de licence qui passe par un serveur situé de l'autre côté de l'Atlantique.

C'est, à sa manière, un document profondément allemand. Sec, ordonné, sans rhétorique. Une défiance méthodique mise en cases, en numéros de critères, en horizons mesurables. SOV-4-09. SOV-6-02-AC. SOV-2-03.

Au-delà du cloud

Et c'est là, peut-être, que C3A devient inspirant bien au-delà du débat sur la souveraineté numérique en Europe.

Car le document n'est pas seulement un référentiel cloud. C'est une grammaire de la résilience, applicable à toute infrastructure critique dont la continuité dépend d'un acteur que l'on ne contrôle pas entièrement. Énergie. Télécommunications. Transports. Santé. Logiciels métiers, modèles d'IA, composants embarqués, chaînes d'approvisionnement industrielles. Partout où une chaîne de valeur traverse une frontière juridique ou capitalistique, la même question se pose, et la même méthode peut s'appliquer.

Quels sont les paramètres mesurables de notre autonomie ? Combien de temps tenons-nous sans le partenaire ? Quelle est la fraîcheur des sauvegardes que nous contrôlons réellement ?

Disposons-nous, sur notre sol, des compétences pour reconstruire, pour patcher, pour signer ? Avons-nous testé, au moins une fois par an, le mode dégradé ? Avons-nous, dans un coffre, la procédure de reprise, et le format dans lequel cette reprise est effectivement exploitable par un autre opérateur que celui qui détient aujourd'hui le système ?

C3A propose un cadre pour répondre à ces questions. Pas en théorie : par numéros de critères, avec des chiffres, des durées, des seuils. C'est ce qui le rend exportable. Un opérateur d'énergie peut s'en inspirer pour ses systèmes de conduite. Un groupe hospitalier peut s'en inspirer pour son système d'information clinique. Un industriel peut s'en inspirer pour la dépendance logicielle de ses lignes de production. Un État peut s'en inspirer pour son socle d'infrastructure numérique tout entier.

Le mérite des Allemands n'est pas d'avoir inventé l'idée. La continuité d'activité, la résilience, la défense en profondeur sont des sujets traités depuis longtemps. Le mérite est d'avoir produit le document. D'avoir transformé une intuition stratégique partagée par beaucoup en une grille de critères sur laquelle on peut se positionner, ligne par ligne. C'est cela qui distingue une doctrine d'une déclaration d'intention : la possibilité d'être audité.

Pour les responsables d'infrastructures critiques (publics ou privés, régulateurs ou opérateurs), C3A vaut moins comme texte que comme modèle. Sa traduction la plus utile n'est pas linguistique. Elle est doctrinale : produire, dans son propre domaine, l'équivalent C3A. Lister les dépendances. Mesurer les délais. Provisionner les compétences. Documenter les procédures. Tester les ruptures. Et inscrire le tout dans un référentiel public que la chaîne des fournisseurs sera bien forcée de prendre au sérieux.

Lu de loin, C3A est un PDF technique. Lu de près, c'est un plan de bataille. Lu pour ce qu'il est, c'est un modèle

reproductible : la démonstration qu’une défiance bien tempérée, soigneusement instrumentée, peut devenir l’un des outils les plus utiles dont disposent les institutions modernes pour protéger ce qui, dans leur fonctionnement, ne doit jamais s’arrêter.

Un aimable correspondant de Souveraine Tech versé dans ces sujets, depuis l’autre bout du monde

---

C3A, oder das methodische Misstrauen

□□ Ende April 2026. Das BSI veröffentlicht ein Dokument von wenigen Dutzend Seiten, frei zum Download auf seiner Website. Nüchterner Titel: *Criteria enabling Cloud Computing Autonomy*. Keine große Pressemitteilung, keine Pressekonferenz. Nur ein PDF, auf den Server gestellt, gezeichnet vom Bundesamt für Sicherheit in der Informationstechnik.

Auf den ersten Blick ein weiteres technisches Dokument in der langen deutschen Tradition cybersicherheitsbezogener Kataloge. C5, IT-Grundschutz, BSI-Standards. Das BSI hat darin Übung. Aber wer C3A genau liest, merkt, dass etwas mit dem üblichen Ton nicht stimmt.

Die Kriterien sind nicht generisch. Sie sind zu präzise.

90 Tage abgekoppelt. Sicherung des Quellcodes alle 24 Stunden, mindestens fünf Versionen. Lokale Ingenieure, die in der Lage sind, einen Notfall-Patch ohne Drittabhängigkeit zu kompilieren und auszuliefern. Ein portables Format für Code, Dokumentation und Verwaltungswerkzeuge, das von der Bundesverwaltung tatsächlich genutzt werden kann. Eine Verteidigungsfall-Klausel, die es dem Staat erlaubt, die

Plattform physisch zu übernehmen.

In einem Zug gelesen, wäre der naheliegende Reflex, von Paranoia zu sprechen. Das Wort kommt schnell, und es ist bequem. Aber es trifft nicht. Was C3A inszeniert, ist keine Pathologie. Es ist methodisches Misstrauen: die kühle, bewusste, dokumentierte Entscheidung, die Kontinuität eines Staates nicht auf den guten Willen eines Anbieters, einer fremden Jurisdiktion oder eines Marktes zu stützen. Misstrauen ist hier keine Stimmung. Es ist eine Disziplin. Und diese Disziplin reicht, wie sich zeigen wird, weit über das Cloud-Thema hinaus.

Ein Konformitätskatalog wird nicht im luftleeren Raum geschrieben. Jedes Kriterium ist die Kristallisation einer Befürchtung, einer praktischen Erfahrung, eines hinter verschlossenen Türen durchgespielten Wargames, aus dem Schlüsse gezogen wurden. Die präzisen Zahlen (90 Tage, 24 Stunden, 5 Versionen) sind keine Beschwörungsformeln. Es sind Parameter. Jemand, irgendwo in den Bonner Büros, hat ein Szenario modelliert, gemessen, wie lange durchzuhalten ist und wie viel Redundanz dafür nötig ist.

Versuchen wir also, den Faden zurückzuverfolgen. Welches Szenario rechtfertigt diese Präzision?

Der Dienstagmorgen

Stellen wir es uns vor.

Dienstagmorgen, kurz vor acht Uhr mitteleuropäischer Zeit. Irgendwo außerhalb der Europäischen Union (die Geographie ist nebensächlich, die Asymmetrie genügt) fällt eine politische Entscheidung. Sie kommt nicht sofort in die Schlagzeilen. Sie nimmt die Form einer Verwaltungsanordnung an, einer Behördenentscheidung, eines von einem Staatssekretär unterzeichneten Schreibens. Der Inhalt ist trocken: Ein in dieser Jurisdiktion ansässiger Cloud-Anbieter wird angewiesen, einen bestimmten europäischen Staat ganz oder teilweise nicht

mehr zu bedienen. Der angegebene Grund (Sanktionen, nationale Sicherheit, Exportkontrolle) ändert nichts an der Mechanik. Die Anordnung ist im Herkunftsland des Anbieters legal. Der Anbieter muss gehorchen.

Um 8:17 Uhr laufen die ersten Alarmmeldungen in den betroffenen Ministerien in Berlin auf. Eine Verwaltungskonsole antwortet nicht mehr. Ein föderierter Authentifizierungsdienst verweigert neue Sitzungen. Ein Cluster wechselt ohne erkennbaren technischen Grund in den Lesezugriffsmodus. Die Betriebsteams öffnen ein Ticket. Das Ticket bleibt unbeantwortet.

Um 9:12 Uhr kommt ein Anruf von der europäischen Tochter des Anbieters. Die Stimme am anderen Ende ist verlegen. Die Teams am Hauptsitz haben Anweisung erhalten, den Kontakt abzubrechen. Die europäischen Ingenieure (formal angestellt bei einer europäischen Einheit, in Euro bezahlt, lebend in München, Dublin, Paris) hatten nie Commit-Rechte am Produktionscode. Sie hatten nie die Signaturschlüssel. Die Control Plane, die sie täglich bedienen, wird aus Seattle oder Redmond gesteuert. Und an diesem Morgen antwortet weder Seattle noch Redmond.

Um 10:30 Uhr beginnt die Krisensitzung. Am Tisch: Beamte des BMI, des BSI, ministerielle Betreiber, Juristen. Sie entdecken, oder erinnern sich an, drei Dinge. Erstens: Die Control Plane ist außer Reichweite und bleibt es, solange die politische Anordnung nicht aufgehoben wird. Zweitens: Die lokal laufenden Binaries funktionieren vorerst weiter, aber die nächste Cloud-Lizenzvalidierung ist in 72 Stunden geplant, und niemand kann vorhersagen, was dann passiert: stille Degradierung, Umschalten in den Demo-Modus, schlichte Abschaltung. Drittens: Wird in dieser Woche eine kritische Schwachstelle bekannt (ein Zero-Day in einer weit verbreiteten Komponente), gibt es auf europäischem Boden niemanden, der den Patch produzieren und ausliefern kann. Die Build-Pipelines liegen beim Anbieter. Die Signierer ebenfalls.

Am Nachmittag beginnt die Schadensaufnahme. Die Gehaltsabrechnung der Beamten des Freistaats Bayern läuft über einen bei diesem Anbieter gehosteten Dienst. Das Aufnahmesystem mehrerer Universitätskliniken auch. Ein Teil der Logistik der Bundeswehr (nicht eingestuft, aber für den Alltag kritisch) ebenfalls. Das Steuer-IT-System teilweise. Das Bürgerportal für die Passverlängerung. Die Anwendung zur Kontrolle der Landgrenzen. Die Austauschplattform zwischen Bund und Ländern.

Am Mittwoch sprechen die Medien von diplomatischen Spannungen. Hinter verschlossenen Türen wird über etwas anderes gesprochen. Über die staatliche Kontinuität. Über die Beamten, die am Freitag bezahlt werden müssen. Über die Patienten, die heute Abend aufgenommen werden müssen. Über die Pässe, die diese Woche verlängert werden müssen. Über Dinge, die nicht auf die diplomatische Lösung einer Krise warten, die Wochen, Monate dauern oder sich in ihrer ursprünglichen Form nie auflösen wird.

Am Donnerstag wird die operative Frage zum ersten Mal laut ausgesprochen. Nicht „wie bekommen wir den Zugang zum Dienst zurück ». Sondern „wie betreiben wir diesen Dienst ohne sie ». Und darüber hinaus: „Wenn die Lage sich verschärft und der Verteidigungsfall ausgerufen wird, sind wir in der Lage, in die Rechenzentren in Frankfurt und Berlin zu gehen, die Schlüssel zu nehmen und diese Plattform selbst zu betreiben (mit unseren Ingenieuren, unseren Werkzeugen, unserem Code) so lange wie nötig? »

In genau diesem Moment entdeckt man, dass die Antwort vollständig davon abhängt, was zuvor vorbereitet wurde.

Und genau hier kommt C3A ins Spiel.

Derselbe Dienstag, aber nach C3A

Spielen wir die Sequenz erneut durch. Derselbe Dienstag. Dieselbe Anordnung von außen. Dieselbe zum Schweigen gebrachte

europäische Tochter. Diesmal aber haben der Kundenstaat und der ihn bedienende Anbieter die letzten zwei Jahre damit verbracht, sich an C3A anzupassen.

Um 8:17 Uhr laufen die ersten Alarmmeldungen auf. Aber sie laufen in einer Umgebung auf, in der das SOC in Deutschland sitzt, von deutschen Ingenieuren betrieben wird, die keine Anweisung aus Seattle erhalten haben, weil sie nicht von Seattle abhängen. Die beobachtete Trennung wird als das interpretiert, was sie ist: ein externes Signal, kein interner Ausfall. Der Krisenstab wird um 8:30 Uhr einberufen: nicht, um zu verstehen, was geschieht, sondern um zu entscheiden, in welchem Tempo ein bereits existierender Plan aktiviert wird.

Um 9:00 Uhr fällt die Entscheidung: Der entkoppelte Modus wird ausgelöst. Nicht in Panik, sondern nach einem dokumentierten, jährlich getesteten Verfahren, wie es SOV-4-09 verlangt. Alle Netzverbindungen zu Nicht-EU-Entitäten werden kontrolliert gekappt. Heartbeats, Lizenzvalidierungsserver, Update-Kanäle, Telemetrie-Ströme. Nichts geht mehr raus, nichts mehr rein. Die Plattform schließt sich um sich selbst und funktioniert weiter.

Sie kann weiter funktionieren, weil der Quellcode, der sie betreibt, in der EU gesichert ist, weniger als 24 Stunden alt, in mindestens fünf Versionen, in einem Format, das die lokalen Ingenieure kompilieren können. Weil diese Ingenieure existieren (SOV-6-02-AC verlangt es): Spezialpersonal auf europäischem Boden, mit lokalen Build-Umgebungen, die Sicherheits-Notfall-Patches ohne externe Abhängigkeit produzieren können. Weil die Schlüssel zur Verschlüsselung sensibler Daten nie in der Umgebung des Anbieters lagen: SOV-3-02 und SOV-3-05 schrieben es vor. Der Anbieter konnte sie selbst dann nicht ausliefern, wenn er dazu gezwungen worden wäre. Sie sind beim Kunden geblieben, in dessen eigenem HSM, auf dessen eigenem Boden.

Um 10:30 Uhr beginnt die Krisensitzung. Aber es ist kein

Krisenstab im dramatischen Sinne mehr. Es ist eine Lagebesprechung. Das SOC bestätigt: Die Dienste laufen. Die Gehaltsabrechnung am Freitag ist gesichert. Die Krankenhäuser nehmen normal auf. Die Pässe werden weiter gedruckt. Der entkoppelte Modus ist darauf ausgelegt, 90 Tage durchzuhalten, der von SOV-4-10 festgelegte Horizont. Neunzig Tage, das ist die Zeit, die eine politische Krise braucht, um sich zu lösen, oder die man braucht, um eine Alternative zu stabilisieren.

Am Mittwoch beginnt das Patching. Eine CVE wird zu einer weit verbreiteten Komponente veröffentlicht. Im Szenario ohne C3A wäre das die Katastrophe gewesen. Hier holen die deutschen Ingenieure den Patch aus den Quellen, kompilieren ihn in ihrer lokalen Build-Umgebung, signieren ihn mit eigenen Zertifikaten, deployen ihn über eine souveräne Pipeline. Es dauert sechsunddreißig statt zwölf Stunden, weil man es nicht gewohnt ist, das allein zu tun. Aber es geschieht.

Am Donnerstag stellt sich die strategische Frage in radikal anderen Begriffen. Nicht „wie lange halten wir durch ». Sondern „wie lange ist es zumutbar durchzuhalten, bevor wir strukturelle Entscheidungen treffen ». Die Wiederaufnahmefähigkeit existiert. SOV-2-03 sieht vor, dass die Bundesverwaltung im Verteidigungsfall Zugriff auf die physischen Anlagen, das Personal, den Quellcode und die Verwaltungswerkzeuge nehmen kann (in portablem Format, das heißt in einer Form, in der ein anderer Betreiber sie tatsächlich betreiben kann). Das Wiederaufnahmepaket wurde vorbereitet. Es liegt im Tresor. Es kann geöffnet werden.

Die am Dienstagmorgen ergangene Anordnung ist nicht verschwunden. Die diplomatische Krise besteht weiterhin. Aber sie diktiert nicht mehr den Rhythmus der Krankenhäuser, der Gehälter, der Grenzen. Die ursprüngliche Asymmetrie (ihr hängt von uns ab, wir hängen nicht von euch ab) wurde durch zwei Jahre methodischer Vorbereitung entwaffnet.

Eine Doktrin, keine Obsession

Liest man C3A nach dieser Übung erneut, ändert sich der Charakter des Dokuments. Es ist kein abstrakter Konformitätskatalog mehr. Es ist die geordnete Bestandsaufnahme einer Doktrin staatlicher Kontinuität gegenüber dem Risiko extraterritorialer Zwangsausübung auf technologischem Wege.

Die Deutschen sagen nicht, dass dieser Dienstag kommen wird. Sie sagen ihn nicht voraus. Sie wünschen ihn nicht. Sie stellen schlicht fest, dass die Möglichkeitsbedingungen dieses Dienstags existieren (in der Konzentration des Cloud-Marktes, in der Extraterritorialität bestimmter Gesetze, in der tiefen Kopplung zwischen den europäischen Operationen und den außereuropäischen Hauptsitzen), und ziehen daraus die Konsequenzen. Pragmatisch. Akribisch. Geordnet.

C3A ist kein optimistisches Dokument. Es ist ein Dokument, das davon ausgeht, dass der gute Wille fremder Jurisdiktionen keine Strategie ist. Dass Souveränität kein Slogan ist, sondern eine Reihe präziser technischer Anforderungen, die sich Punkt für Punkt prüfen lassen. Und dass die staatliche Kontinuität strukturell nicht von einer Lizenzvalidierungsschleife abhängen kann, die über einen Server jenseits des Atlantiks läuft.

Es ist auf seine Art ein zutiefst deutsches Dokument. Trocken, geordnet, ohne Rhetorik. Methodisches Misstrauen, gefasst in Felder, in Kriteriennummern, in messbare Horizonte. SOV-4-09. SOV-6-02-AC. SOV-2-03.

Über die Cloud hinaus

Und vielleicht ist es genau hier, wo C3A weit über die Debatte um die digitale Souveränität in Europa hinaus inspirierend wird.

Denn das Dokument ist nicht nur ein Cloud-Katalog. Es ist eine

Grammatik der Resilienz, anwendbar auf jede kritische Infrastruktur, deren Kontinuität von einem nicht vollständig kontrollierten Akteur abhängt. Energie. Telekommunikation. Verkehr. Gesundheit. Branchensoftware, KI-Modelle, eingebettete Komponenten, industrielle Lieferketten. Überall dort, wo eine Wertschöpfungskette eine juristische oder kapitalbezogene Grenze überquert, stellt sich dieselbe Frage, und dieselbe Methode lässt sich anwenden.

Was sind die messbaren Parameter unserer Autonomie? Wie lange halten wir ohne den Partner durch? Wie aktuell sind die Sicherungen, die wir tatsächlich kontrollieren? Verfügen wir auf unserem Boden über die Kompetenzen zum Wiederaufbau, zum Patchen, zum Signieren? Haben wir mindestens einmal jährlich den degradierten Modus getestet? Liegt im Tresor das Wiederaufnahmeverfahren, und in welchem Format ist diese Wiederaufnahme tatsächlich durch einen anderen Betreiber als denjenigen umsetzbar, der das System heute hält?

C3A schlägt einen Rahmen für die Beantwortung dieser Fragen vor. Nicht in der Theorie: nach Kriteriennummern, mit Zahlen, Zeiträumen, Schwellenwerten. Genau das macht es exportierbar. Ein Energieversorger kann sich daran für seine Leitsysteme orientieren. Ein Krankenhausverbund kann sich daran für sein klinisches Informationssystem orientieren. Ein Industrieunternehmen kann sich daran für die Softwareabhängigkeit seiner Produktionslinien orientieren. Ein Staat kann sich daran für sein gesamtes digitales Infrastrukturfundament orientieren.

Das Verdienst der Deutschen besteht nicht darin, die Idee erfunden zu haben. Geschäftskontinuität, Resilienz, Verteidigung in der Tiefe sind seit Langem behandelte Themen. Das Verdienst besteht darin, das Dokument produziert zu haben. Eine von vielen geteilte strategische Intuition in ein Raster von Kriterien überführt zu haben, an dem man sich Zeile für Zeile messen kann. Genau das unterscheidet eine Doktrin von einer Absichtserklärung: die Auditierbarkeit.

Für Verantwortliche kritischer Infrastrukturen (öffentlich oder privat, Regulierer oder Betreiber) zählt C3A weniger als Text denn als Modell. Seine nützlichste Übersetzung ist nicht sprachlich. Sie ist doktrinal: im eigenen Bereich das C3A-Äquivalent zu erstellen. Die Abhängigkeiten auflisten. Die Fristen messen. Die Kompetenzen vorsorglich aufbauen. Die Verfahren dokumentieren. Die Brüche testen. Und das Ganze in einen öffentlichen Katalog überführen, den die Lieferantenkette zwangsläufig ernst nehmen wird.

Aus der Distanz gelesen ist C3A ein technisches PDF. Aus der Nähe gelesen ist es ein Schlachtplan. Liest man es für das, was es ist, dann ist es ein reproduzierbares Modell: der Beweis, dass ein wohltemperiertes, sorgfältig instrumentiertes Misstrauen zu einem der nützlichsten Werkzeuge moderner Institutionen werden kann, um zu schützen, was in ihrem Funktionieren niemals stillstehen darf.

Ein freundlicher Korrespondent von Souveraine Tech, der sich mit diesen Themen bestens auskennt, vom anderen Ende der Welt