Zusatzmaterial zur Dissertation:

Internationaler Datentransfer zwischen der EU und den USA
Rechtliche und technische Anforderungen auf europäischer und US-amerikanischer Ebene

Dr. Tatia Bagauri

Inhaltsverzeichnis

Anlage 1 – Interview im Rahmen des Datenschutzes

Cornelia Sasse
Group Data Protection Officer
Wird interviewt am 17.02.2023

Dr. Tatia Bagauri: – Am 07.10.2022 wurde in den USA ein Dekret / Executive Order (E. O. 14086) erlassen. Ändert sich mit dieser Order zur Umsetzung des Privacy Shield 2.0 etwas an der aktuellen Regelung bezüglich der Standarddatenschutzklauseln? Kann man sich dieses Mal darauf verlassen, dass die USA die oben beschriebenen Einschränkungen einhalten und die vom EUGH aufgegriffenen Kritikpunkte entsprechend umsetzen?

Cornelia Sasse: – Nach meiner Einschätzung wird die E. O. nicht wirklich etwas an der Regelung bezüglich der Standardvertragsklauseln ändern. Die E. O. ist auf die Massenüberwachung durch US-Geheimdienste fokussiert. Der US-Präsident definiert darin einen zweistufigen Rechtsschutz-mechanismus, wobei die erste Stufe dem bisherigen Ombudspersonen-Mechanismus ähnelt. In der zweiten Stufe wird der neu etablierte Data Protection Review Court angehört, der allerdings keine echte Judikative ist. Es bleibt abzuwarten, ob der EuGH dieses Gremium akzeptiert. Ferner werden die in beiden Stufen getroffenen Entscheidungen geheim bleiben, was auch gegen den Fair-Trial-Grundsatz nach Art. 6 Europäische Menschenrechtskonvention verstoßen wird.

Dr. Tatia Bagauri: – Eine E. O. Beruht ausschließlich auf einer Entscheidung des amtierenden US-Präsidenten. Sie kann nicht durch den US-Kongress außer Kraft gesetzt werden. Sollte der US-Präsident aber die nächsten Präsidentschaftswahlen verlieren, kann sein Nachfolger diese Verordnung aufheben oder ändern. Kann dies Auswirkungen auf den Datenschutz haben? Sehen Sie eine rechtliche Gefahr dahinter?

Cornelia Sasse: – Die Vergangenheit hat gezeigt, dass sich jegliche US-EU Verhandlungen im Datenschutz sehr zäh gestaltet und jahrelang gedauert haben. So sehe ich persönlich es auch im oben beschrieben Fall als vorhersehbar an, dass ein Regierungswechsel hier zu weiteren Verzögerungen bzw. Unsicherheiten im internationalen Datentransfer führen kann. Von rechtlichen Gefahren möchte ich nicht sprechen, aber Risiken sehe ich schon, die durch die Unsicherheit der Vertragspartner aufgrund fehlender Rechtssicherheit entstehen können. (z. B. analog den Unsicherheiten, die im Zusammenhang mit der Anwendung des Privacy Shield herrschten).

Dr. Tatia Bagauri: – Standarddatenschutzklauseln der Aufsichtsbehörde bedürfen zwar der Genehmigung durch die Europäische Kommission, fallen aber nach der juristischen Literatur unter die Kategorie der nicht genehmigungspflichtigen Garantien. Würden Sie sie als solche klassifizieren, oder fallen sie Ihrer Meinung nach unter die genehmigungspflichtigen Garantien?

Cornelia Sasse: – Die EU-Kommission gibt die Muster der Standardvertragsklauseln heraus und stellt sie den Unternehmen in der EU zur Verfügung. Solange diese an den Klauseln in ihren Individualverträgen nichts verändern, bedarf es m. E. keiner Genehmigung durch einzelne Aufsichtsbehörden. Dieses Erfordernis sehe ich nur bei Abweichungen vom EU-Standard, so ist es auch vorgesehen. Schließlich werden die Standardvertragsklauseln der EU von kompetenten Datenschutzgremien, in welchen auch Aufsichtsbehörden vertreten sind, entworfen und beschlossen.

Dr. Tatia Bagauri: – Genehmigte Verhaltensregeln (CoC) aus Art. 40 DSGVO dienen als Nachweis der Einhaltung datenschutzrechtlicher Pflichten aus der DSGVO. Obwohl CoC für kleinste, kleine und mittlere Unternehmen vorgesehen sind, zeigt sich in der Praxis häufig, dass sie nicht eingeführt bzw. vorhanden sind. In den USA gibt es keine Vorschrift, dass CoC in einer Organisation eingeführt werden muss. Wie wichtig sind sie Ihrer Meinung nach? Für wie wichtig halten Sie diese? Wenn eine Organisation sie nicht niederschreiben möchte oder gesetzlich nicht dazu verpflichtet ist, was sehen Sie dann als Alternative?

Cornelia Sasse: – Ich würde es nicht für grundsätzlich erforderlich halten, dass jedes Unternehmen einen CoC einführt. Aber für Branchen, die mit sensiblen Daten oder aber großen Datenmengen arbeiten, halte ich die CoC als besonderes vertrauensbildendes Instrument. Alternativ sehe ich die Zertifizierung einzelner Unternehmensbereiche / Verarbeitungen als sinnvoll an (s. Antwort zu den folgenden Fragen).

Dr. Tatia Bagauri: – Derzeit existieren keine konkreten CLOUD Act- oder CCPA-Zertifizierungen. Welche Rolle werden angemessene Zertifizierungen im Rahmen der DSGVO, des CLOUD Acts oder des neuen EU-US Data Privacy Framework spielen, wenn sie gesetzlich vorgeschrieben sind und verlangt werden?

Cornelia Sasse: – Ich halte es für sehr kritisch, Zertifizierungen für alle Unternehmen gesetzlich vorzuschreiben. Hier sehe ich eine große Gefahr, dass sich der Großteil der kleinen und mittelständischen Unternehmen diese Zertifizierungen weder finanziell noch ressourcenmäßig überhaupt leisten können. Sollen diese Unternehmen dann benachteiligt werden? Eine gesetzlich erzwungene Zertifizierung ist m. E. überdimensioniert. Sinnvoll halte ich Zertifizierungen für Branchen, die mit sensiblen Daten oder großen Datenmengen umgehen bzw. risikoreiche Datenverarbeitungen durchführen. Hier wäre die Zertifizierung des entsprechenden Unternehmensbereiches wünschenswert. Eine Zertifizierung über alle Geschäftsbereiche eines Unternehmens halte ich für nicht erforderlich und auch nicht für sinnvoll. Wichtig wäre es, dass der Unternehmensbereich, in welchem die besondere Datenverarbeitung stattfindet, zertifiziert ist.

Dr. Tatia Bagauri: – Auf europäischer Ebene sind Privacy by Design und Privacy by Default gesetzlich verankert. In den USA ist nur der erste Grundsatz bekannt und wird angewandt. Wie wichtig ist Privacy by Default für die rechtmäßige Verarbeitung bzw. Übermittlung von Daten? Kann Privacy by Design als Ausgleich zu Privacy by Default gesehen werden oder ist seine Nichtexistenz als ein Mangel im amerikanischen Rechtssystem zu bewerten?

Cornelia Sasse: – Beide Ansätze gehören für mich zusammen. Privacy by Design meint die Berücksichtigung aller Datenschutzanforderungen bereits bei der Planung einer Verarbeitung oder Herstellung einer Software. Mit Privacy by Default werden die datenschutzfreundlichen Einstellungen dann vor der Nutzung direkt im Tool vorgenommen. Für mich bedeutet ein starkes Privacy by Design später weniger Aufwände für die Gestaltung der Privacy by Default. Je besser ein Unternehmen also bereits plant, desto einfacher und rechtssicherer ist die datenschutz-freundliche Anwendung später.

Die meisten Unternehmen, egal ob US oder EU, fokussieren m. E. jedoch viel zu sehr auf den Einstellungen zur (physischen) Datensicherheit als zur datenschutzrechtlichen Sicherheit der Betroffenen. Die Abbildung der Betroffenenrechte ist immer noch eine große Lücke in den meisten Anwendungen. Hier herrscht m. E. überall Nachbesserungsbedarf und vor allem das Verständnis darüber, dass der Datenschutz die Rechte der Betroffenen behandelt und die Daten- oder Informationssicherheit den tatsächlichen Schutz der Daten selbst meint. Wäre dies Verständnis US- und EU-weit ausgeprägter, müsste über Privacy by Design und Privacy by Default gar nicht diskutiert werden.

Anlage 2 – Interview im Rahmen der Informationssicherheit

Dr. Florian Wrobel

Managing Director bei COGITANDA Risk Prevention GmbH
Wird interviewt am 12.02.2023

Dr. Tatia Bagauri: – Wenn man die Informationssicherheit betrachtet, stellt man fest, dass sie das gleiche Ziel verfolgt wie die Datensicherheit. Kann dadurch festgelegt werden, dass beide deckungsgleich sind oder weisen sie unterschiedliche Feinheiten auf?

Dr. Florian Wrobel: – Schon eine entspannte Frage zum Start. In der Praxis werden sie als Synonyme verwendet. Meines Erachtens sind sie nicht dasselbe, auch wenn ich manchmal schuldig bin und sie als Synonyme nutze. Daten sind m. E. die einzelne Einheit, Wissen oder Now How. Sie sind vor allen Dingen technisch und werden als z. B. Bytes, Megabytes oder Gigabytes gespeichert. Das bedeutet, dass wir in erster Linie über IT sprechen.

Der Begriff „Informationssicherheit“ ist m. E. weiter gefasst. Informationen kommen in vielen verschiedenen Varianten vor. In der Informationssicherheit machen wir uns z. B. Gedanken, dass, wenn wir telefonieren, nicht jemand das Gespräch überhört. Es sind dann Informationen, die wir zwar aus irgendwelchen Daten abgeleitet haben und nicht Daten. Wissenschaftlich gesehen, Datensicherheit ist ein Bestandteil der Informationssicherheit. Informationssicherheit ist der größere oder weiter gefasste Begriff, wobei auch das gesprochene Wort zu schützen ist.

Dr. Tatia Bagauri: – Es ist ein sehr guter Punkt, den Sie erwähnen. Mit der Informationssicherheit meinen wir auch die Art der Übertragung der Informationen und die beteiligten Personen, die die Informationen transferieren. Das ist eine gute Überleitung zu der anderen Frage. Was sollten das Ziel und die Mittel der Schulung / Sensibilisierung der Mitarbeiter bezüglich des Datentransfers sein und worauf sollte geachtet werden? Welche Rolle kann ein geschulter Mitarbeiter bei der Datenübermittlung spielen?

Dr. Florian Wrobel: – Sicherstellung der Informationssicherheit ist ein wesentlicher Aspekt für ein Unternehmen, Strafen zu vermeiden. Wir brauchen Compliance mit einschlägigen Gesetzen und die Non-Compliance ist eines der wesentlichen Informationssicherheitsrisiken. Der Datentransfer (international bzw. nicht international) oder die ungewollte Veröffentlichung sind die Themen, wobei der Mitarbeiter viel falsch machen kann, so dass er darüber zu schulen ist.

Jetzt ist die Frage, wie schult man den Mitarbeiter. Man braucht einen Dreiklang. 1. Die Kommunikation: Die Erwartungen und die Anforderungen müssen klar kommuniziert werden; im besten Fall in Form einer Richtlinie oder Anweisung. 2. Das Training: D. h. ihm die Werkzeuge an die Hand zu geben, die er braucht, um im Einklang mit einschlägigen Gesetzen mit Daten und Informationen umzugehen. 3. Abhängig vom Thema (es wäre aber für das Thema ,,Datenübertragung“ nicht so relevant): Übung und Simulationen.

Für das Thema ,,Datenübertragung“ braucht eine Organisation eine angemessene Kommunikation und angemessenes Training, nicht nur einmal, sondern regelmäßig, um das reale Risiko, dass der Mitarbeiter dort etwas falsch macht, was zu einem Gesetzesverstoß führt, zu reduzieren.

Dr. Tatia Bagauri: – Halten sich Mitarbeiter nicht an die Informationssicherheitsrichtlinie, müssen disziplinarische Maßnahmen abgeleitet werden. Was wäre Ihrer Meinung nach effektiver: Disziplinarmaßnahmen, ein Belohnungssystem oder eine Kombination aus beidem?

Dr. Florian Wrobel: – Auch eine sehr spannende Frage! Meines Erachtens ist die Security Community diesbezüglich nicht wirklich einig. Für mich ist ein Verstoß gegen Informationssicherheitsrichtlinien, inklusive Richtlinien für die Datenübertragung, genauso einzuordnen wie Diebstahl, Arbeitsverweigerung oder am Arbeitsplatz schlafen. Wir würden nicht auf die Idee kommen, einen Mitarbeiter zu belohnen, weil er z. B. nicht stiehlt. Kein Mensch würde darüber nachdenken. Deswegen wäre ich absolut für disziplinarische Maßnahmen. Das müssen wir jetzt aber relativieren.

Wenn der Mitarbeiter einen Fehler bei der Datenübertragung macht und es zu einem Gesetzesverstoß oder Datenschutzvorfall kommt, dann sag ich nicht, der Mitarbeiter muss sofort abgemahnt werden. Man muss die Ursachenforschung durchführen. Es kann sein, dass man feststellt, dass man den Mitarbeiter nicht vernünftig trainiert hat bzw. die Erwartungen nicht angemessen kommuniziert hat. Nichtsdestotrotz bleibe ich dabei, dass Disziplinarmaßnahmen erforderlich sind. In dem Beispiel wäre der erste Schritt, aus meiner Sicht, ein Gespräch mit der Führungskraft zu führen, um mögliche Wissenslücken nachzuarbeiten. Aber wenn der Mitarbeiter, der ein Gespräch mit der Führungskraft hatte, kurze Zeit später oder in dem selben Jahr denselben Fehler macht, musste man über weitere Maßnahmen nachdenken. Wenn der Mitarbeiter denselben Fehler immer und immer wieder macht, würde es sicherlich irgendwann zu Abmahnung und Kündigung kommen.

Dr. Tatia Bagauri: – Welche Rolle kann die organisatorische Ausgestaltung des Konfigurationsmanagements bei dem Datentransfer spielen, und was ist dabei besonders zu beachten?

Dr. Florian Wrobel: – Was ich immer für organisatorische Regelungen zu dem Ganzen empfehle, ist ein Dokument, wie eine Richtlinie oder Leitlinie zum Thema Härtung von IT-Systemen / „Hardening“, zu erlassen. Wenn man ein Stück Hardware kauft, wie einen neuen Router oder Server, erhält man häufig z. B. Passwörter mitgeteilt. Da sind wir uns einig, dass solche Passwörter zu ändern sind. Wie wollen wir sicherstellen, dass der Mitarbeiter in der IT es auch umsetzt? Möchten wir eingeben, dass es für ihn selbstverständlich ist? Er bräuchte dann so ein Dokument nicht? Für andere aber vielleicht nicht. Von daher müssen IT- Maßnahmen, aus meiner Sicht, immer organisatorisch begleitet werden, um sicherzustellen, dass wieder dasselbe Ergebnis erzeugt wird.

Nur durch das Blatt Papier hat man die Sicherheit natürlich nicht, aber es ist der erste Schritt. Wir können nur dann von den Mitarbeitern erwarten, dass sie sich korrekt verhalten, inklusive die Mitarbeiter in der IT, die die Systeme konfigurieren oder Updates einspielen, wenn klar formuliert ist, was hier erwartet wird.

Dr. Tatia Bagauri: – Ich hätte eine ergänzende Frage dazu. Sollte man erstmal vorschreiben, was man umsetzen möchte und dann implementieren oder umgekehrt? Wie Sie skizziert haben, wäre erstmal alles niederzuschreiben und nachher umzusetzen, richtig?

Dr. Florian Wrobel: – Genau! Das sehe ich so. Der Chief Information Security Officer (CISO) kann formulieren, wie ein angemessenes Sicherheitsniveau aussieht. Im beruflichen Alltag redet man natürlich am besten mit der IT. Es macht keinen Sinn, etwas in den Richtlinien zu schreiben, was komplett unrealistisch ist. Es wird dann trotzdem nicht gemacht.

Logischerweise macht es auch keinen Sinn, Richtlinien zu erlassen und nicht zu kontrollieren. Also wenn es um das Thema Systemkonfiguration geht, sollte in irgendeiner Form überprüft / auditiert werden. Es sollte ein Reporting / Monitoring geben, um sicherzustellen, dass es auch gemacht wird.

Dr. Tatia Bagauri: – Welches Tool bzw. Instrument soll eine Organisation implementieren bzw. was soll eine Organisation tun, wenn sie Datenlecks vermeiden und ihnen entgegenwirken möchte?

Dr. Florian Wrobel: – Wenn man wirklich den unautorisierten Teil von Informationen stoppen will, braucht es ein DLP-System / „Data Loss Prevention“; „P“ wirklich für die Prävention. Es sind Systeme, die, basiert auf einer gewissen Logik, gewisse Aktionen stoppen. Zum Beispiel, man kann dem System beibringen, dass Kreditkartendaten per E-Mail oder per Chat-Nachricht nicht weitergeleitet werden dürfen. Wenn man dann eine E-Mail mit einer Kreditkartennummer schreibt, wird es unmöglich, diese abzusenden. Man erhält eine Warnmeldung: „Achtung! Es ist nicht erlaubt!“ Solche Systeme können in allen Dokumenten hochgehen und wenn das Dokument die Kreditkartennummer beinhaltet, kann man das Dokument nirgendwo hochladen. Es ist technisch, aus meiner Sicht, die einzige Möglichkeit, Datenlecks wirklich zu unterbinden.

Die Information oder, in diesem Fall, Daten, sind auf IT-Systemen gespeichert und man kann auch versuchen, sie in irgendeiner Form zu unterschreiben, zu beschreiben und damit technische Aktionen zu unterbinden. Aber wenn der Mitarbeiter, der ein Blatt Papier irgendwo mitnimmt, sind dies auch Informationen, die geleakt werden können. Interne E-Mails können ausdruckt werden. Das Drucken könnte man mit dem DLP-System unterbinden, aber wenn man nicht daran gedacht hat und der Mitarbeiter etwas ausdruckt und an Wikileaks sendet, dann ist es weg und dann kann man es nicht mehr stoppen. Der Mitarbeiter kann auch den Telefonhörer in die Hand nehmen, um Betriebsgeheimnisse auszuplaudern. Also hundertprozentige Gewissheit gibt es leider nicht. Man kann aber einiges tun, um die Mitarbeiter zu schulen / um sie wissen zu lassen, was die Erwartung ist und was Konsequenzen sind, wenn sie sich nicht daran halten. Dazu ein gut konfiguriertes DLP-System setzt voraus, dass man seine Daten und Informationen kennt, sie genau beschrieben hat und basierend darauf gewisse Regeln erlässt, was mit diesen Daten passiert oder nicht.

Dr. Tatia Bagauri: – Gemäß ISO 27001: A.8.13 soll das Thema „Backups“ in einer Richtlinie thematisiert werden. Darüber hinaus sollen Backups regelmäßig getestet werden. Warum ist es wichtig, dieses Thema in einer Richtlinie zu behandeln und warum sollten sie regelmäßig getestet werden? Was genau soll „Regelmäßigkeit“ in diesem Fall bedeuten?

Dr. Florian Wrobel: – Ein wichtiger Schutzwert in der Informationssicherheit ist die Verfügbarkeit. Es gibt verschiedene Szenarien, wie die Verfügbarkeit beeinträchtigt wird. Insbesondere Verschlüsselungsangriffe durch Hacker, die sämtliche IT-Systeme und die Daten, die dort gespeichert sind, verschlüsselt, entziehen dem Unternehmen den Zugriff auf diese Daten, und damit kann es seinen gesetzlichen Pflichten nicht mehr nachkommen. Hier spielt das Backup die entscheidende Rolle. Nur durch eine vernünftige Datensicherung, die belastbar ist, kann man sicherstellen, dass die Verfügbarkeit gewährleistet ist.

Die Datensicherung ist leicht gesagt, muss aber richtig gemacht werden. In der Regel gehören die Daten nicht der IT, sondern zu einer Geschäftseinheit. Sie müssen sich darüber Gedanken machen, wie viele Stunden, Tage oder Wochen sie die Daten verlieren können und was der Impact wäre, wenn sie die Daten verlieren. Daraus abgeleitet, wird festgelegt, wie häufig man die Daten sichert.

Wie wir skizziert haben, muss schriftlich fixiert werden, was überhaupt die Erwartungshaltung ist. Um ein angemessenes Schutzniveau zu haben und die Datensicherung zu schützen, so dass nicht die Datensicherung angegriffen wird, muss beschrieben werden, was erwartet wird. Das macht man in der Form von Richtlinien, IT setzt um und die Umsetzung wird überprüft.

Ich habe es bereits angesprochen, wie wichtig eine belastbare Datensicherung ist. Wenn ich nicht weiß, dass ich Daten aus der Datensicherung wiederherstellen kann, habe ich keine belastbare Datensicherung. Man muss die Daten auch wieder ausblenden können, sonst wird das eigentliche Ziel nicht erreicht. Man muss testen, die Daten wiederherzustellen. Damit wird festgestellt, dass sie funktionieren und man sich auf diese Medien verlassen kann.

Dr. Tatia Bagauri: – Gibt es dafür einen bestimmten Zeitraum, wann oder wie oft sie getestet werden sollten, oder ist es von der Organisation abhängig?

Dr. Florian Wrobel: – Hier ist es schwer, etwas pauschal zu sagen. Es ist risikobasierend. Immer wenn ich etwas neu mache, z. B., wenn ich das Datensicherungskonzept ändere oder von Bandlaufwerken auf den Cloud Anbieter wechsele, sollte ich es am besten, bevor ich die Laufwerke abschalte, einmal testen. Ansonsten würde ich sagen mindestens jährlich. Alles andere ist nicht unbedingt zielführend.

Dr. Tatia Bagauri: – ISO Norm beschreibt den PDCA-Zyklus. Wenn diese Ziele in der Planungsphase bei PDCA-Zyklus nicht klar beschrieben wären, wäre es möglich, dies in der Check-Phase zu tun? Wäre das dann wieder die Check-Phase oder beginnt man wieder mit der Planungsphase neu?

Dr. Florian Wrobel: – Genauso! Check ist genau dafür da. Dort schaut man sich an, wie wirksam die Maßnahmen sind. Alles, was nicht wirksam ist, beginnt wieder von vorn, wie man alternative Umsetzungen plant, was man nach der Umsetzung im nächsten Check wieder überprüft. So dreht man sich immer und immer wieder im Kreis. Man ist nie fertig, weil es immer Verbesserungspotenzial gibt. Im Check werden Abweichungen aufgedeckt, deren Behebung im Plan geplant und im Do umgesetzt werden.

Dr. Tatia Bagauri: – Ist die Act-Phase beim PDCA-Zyklus vollständig von der Check-Phase abhängig, oder sehen Sie sie eher als die Zusammenfassung aller drei vorherigen Phasen?

Dr. Florian Wrobel: – Gewisse Dinge müssen nach Umsetzung erstmal laufen. Also es ist nicht so, dass es sofort nach dem Do überprüft wird. Im Managementsystem ist jedoch das Hauptmittel für einen Check ein Audit, entweder durch einen unabhängigen Dritten oder durch interne Ressourcen (ein internes Audit). Man hat also einmal im Jahr die Check-Phase. Dadurch wird überprüft, ob das Sicherheitsniveau, was definiert wurde, tatsächlich erreicht wird. Da kommen Abweichungen heraus oder Verbesserungspotenziale, die wieder umgesetzt werden.

Viel hängt von der Kritikalität ab. Wenn etwas Kritisches ist, weiß man, was man erwarten soll. Bei den allermeisten Abweichungen lässt man sich bestätigen, dass es umgesetzt wurde (d. h. Do). Wenn es umgesetzt ist, dann nimmt man das als gegeben hin und wenn man das nächste Audit plant, macht man es wieder.

Dr. Tatia Bagauri: – Auf welche Ereignisse soll geachtet werden, wenn ein Sicherheitsvorfall als Informationssicherheitsvorfall bewerten wird? Können Sie ein paar Beispiele nennen?

Dr. Florian Wrobel: – Es ist wichtig erstmal ein vernünftiges Informationssicherheitsvorfall-Management / „Information Security Incident Management“ zu haben.

Etablieren: typischerweise bedeutet dies, dass wir den Mitarbeitern beibringen müssen, sämtliche Vorfälle (das inkludiert auch Verdachtsfälle) zu melden. Das ist das Entscheidende. Dann gibt es IT-Vorfälle / IT-Incidents. Zum Beispiel, der Mitarbeiter meldet sich: „Mein Computer funktioniert nicht mehr, mein Monitor ist schwarz, die Festplatte ist kaputt, das Netzteil ist durchgeschmort.“ Auch Hardware geht kaputt. Dies sind typische IT-Vorfälle, die von der IT zu managen sind. Wenn der Mitarbeiter sich meldet, dass sein Monitor schwarz ist, könnte es aber auch sein, dass der Rechner mit einer Malware infiziert wurde und der PC deswegen nicht funktioniert. Dann ist es natürlich ein Informationssicherheitsvorfall. Wenn im weiteren Verlauf festgestellt wird, dass die Malware nicht nur die Funktion beeinträchtigt hat, sondern Daten an den Hacker geschickt hat und es auch personenbezogene Daten waren, dann ist es ein Datenschutzvorfall.

Der typische Weg, den es braucht, ist der Folgende: Allen Mitarbeitern erklären, alles zu melden; lieber einmal mehr melden als einmal zu wenig. Dann wird typischerweise in der IT eine Stelle eingerichtet, wo diese Vorfälle ankommen. Die Personen, die solche Vorfälle und Verdachtsfälle initial annehmen, brauchen eine organisatorische Regelung, wie damit umzugehen ist. Wie gerade skizziert, es gibt ganz einfache IT-Vorfälle. Da muss man nichts weiter machen. Die IT kann sich darum kümmern: Ein neues Netzteil aus dem Lager nehmen oder neuen Rechner verschicken, damit der Mitarbeiter wieder arbeiten kann. Darüber hinaus existieren weitere Maßnahmen. Es gibt Anweisungen, die erlassen werden müssen, welche Schritte zur Untersuchung vorzunehmen sind.

Wenn man mehr Informationen bekommt, dann wird aus einem Verdachtsfall ein echter Informationssicherheitsvorfall. Wenn diese Erkenntnis da ist, muss es ein Meldewesen geben. Zum Beispiel muss CISO informiert werden. Wenn personenbezogene Daten involviert sind, muss der Datenschutz involviert werden. Um sicherzustellen, dass jeder Vorfall immer gleich zu bewerten ist, muss es ein Schema geben. Die klare Regelung der Klassifizierung muss man dem Helpdesk / Servicedesk mitgeben. Je nachdem wie kritisch die Situation ist, muss die Geschäftsführung informiert werden.

Dr. Tatia Bagauri: – Könnten Sie bitte kurz skizzieren, wie die Meldung an die zuständige Behörde weitergeleitet bzw. wie die zuständige Behörde über einen Informationssicherheitsvorfall informiert wird? Was wären die wichtigsten Schritte und Prozesse, die zu unternehmen sind?

Dr. Florian Wrobel: – Hier sehe ich die einzelnen Rollen im Incident-Management-Prozess in der Verantwortung, die geregelt werden müssen. Die DSGVO stellt 72 Stunden Meldefrist klar. Das ist nicht das Problem für CISO bzw. Informationssicherheit. Das Thema wird sich aber ab dem nächsten Jahr ändern. In NIS 2 und DORA (insbesondere in NIS 2) stehen neue Anforderungen, um Cyber- Angriffe zu melden.

Folgendes muss im Unternehmen geregelt werden: Wer gibt die Meldung ab? Ist es das, was der ISB bzw. CISO übernehmen darf? Soll die Compliance, Legal Abteilung und Geschäfts-führung involviert werden? Das Schema ist die eine Sache; den jeweiligen Rollen, klare Aufgaben und Verantwortlichkeiten zuzuordnen, ist der nächster Schritt. Da gehört die Meldung dazu. Darüber hinaus müsste die Cyber-Versicherung informiert und müssten IT-Forensiker eingeschaltet werden. Wird aus einem Incident ein echter Notfall bzw. eine Krise, muss der Krisenstab informiert werden. Daher muss klar geregelt werden, wer das eigentlich macht.

Derzeit müssen KRITIS-Unternehmen in Deutschland beim BSI melden. Heute bekommen wir sicherlich nur die Hälfte mit. Was in den Medien ist, ist nur ein Bruchteil der Vorfälle, die tatsächlich passieren.

Dr. Tatia Bagauri: – Also ist es derzeit so, dass ein Unternehmer sich beim BSI nur dann melden soll, wenn es KRITIS-relevant ist?

Dr. Florian Wrobel: – Genau, es ist tatsächlich klar geregelt. Es gibt einen KRITIS- Beauftragten. Man muss sich beim BSI registrieren. Dort gibt es ein eigenes Portal. Es kann nicht jeder machen, sondern der, der schon in der Verantwortung ist. Er muss natürlich in den Incident-Management-Prozess eingebunden sein.

Dr. Tatia Bagauri: – Bedeutet dies, dass ein Unternehmen, das nicht zu den kritischen Unternehmen gehört, nur dann melden sollte, wenn es sich um einen Datenschutzvorfall handelt?

Dr. Florian Wrobel: – Noch nicht, aber es kommt. Wenn nicht personenbezogene Daten betroffen werden, muss man spätestens ab dem nächsten Jahr melden.

Anlage 3 – Interview im Rahmen der Cybersicherheit

Jan-Henning Evers
Managing Director Global Claims bei COGITANDA Claims Services GmbH
Wird interviewt am 15.02.2023

Dr. Tatia Bagauri: – Im Bereich der Cyber Sicherheit ist die Reaktion auf Vorfälle ein wesentliches Element zum Schutz von Daten bzw. Informationen und zur Gewährleistung des Sicherheitsniveaus in der Organisation. Was ist der erste Schritt der Incident Response und worauf sollte in dieser Phase besonders geachtet werden?

Jan-Henning Evers: – Zuerst muss man den Sachverhalt ermitteln und nachher bewerten. Solange sich der Sachverhalt bewegt, kann man ihn nicht bewerten. Es ist immer so! Es ist auch bei einer Soforthilfe so, die man in einem Cybervorfall leistet. Man muss sich immer einen Überblick über die Situation verschaffen, zumindest soweit man es kann und dann seine Maßnahmen und Handlungen ableiten. Ich kann eine perfekt ausgeführte Sofortmaßnahme ausführen, wenn sie aber nicht eine gebotene Sofortmaßnahme ist, weil sie nicht zum Ereignis passt, bringt es nichts. Also erst analysieren, dann nachdenken und dann handeln! Diese Schritte muss man immer machen. Dabei sind die folgenden Punkte zu ermitteln: Was ist passiert? Wem ist das passiert? Wo kommt es her? Warum ist es passiert? Welche Auswirkungen es hat, d. h. auf welche natürlichen oder juristischen Personen, auf eine nur oder auf mehrere Personen oder auf Unternehmen? In einem IT und Cybervorfall gehört dazu, solange verwertbare Spuren da sind, immer einen IT-Forensiker zu involvieren.

Dr. Tatia Bagauri: – Die IT forensische Analyse wäre der erste Schritt / Teil des gesamten Prozesses und nicht der gesamte Prozess selbst, richtig?

Jan-Henning Evers: – Es ist natürlich ein Teil der Arbeit, aber es ist eine Arbeit, die unerlässlich ist. Die IT-Forensiker können in die Vergangenheit schauen. Sie sind in der Lage mit ihren Analysen, in die Systeme zuschauen und nachvollziehen, was passiert ist und wie es zu diesem Vorfall gekommen ist. Es wird mit Artefakten und mit entsprechenden Beweisen gesichert, dass es gerichtsfest ist. Das ist die wesentliche Arbeit des Sachverhalts. Dadurch wird klar gemacht, was passiert ist, und es wird der Sachverhalt nachgebildet.

Aus den ersten Ergebnissen der IT forensischen Untersuchung und damit des Sachverhalts leite ich meine technischen und organisatorischen Handlungen ab. Technische Maßnahme wäre z. B. der Neuaufbau der IT-Infrastruktur oder das Reinigen der aktuellen IT-Infrastruktur. Organisatorische Maßnahme wäre z. B. die Meldung bei der Datenschutzbehörde oder das Umstellen meines Betriebs.

Dr. Tatia Bagauri: – Welche Rolle spielt die IT-Forensik bei der Incident Response und wann sollte sie in den Vorfall eingeschaltet werden?

Jan-Henning Evers: – Die IT-Forensik muss immer involviert werden; ohne eine IT-Forensik geht es nicht, es sei denn der Vorfall liegt so lange zurück, dass keine forensisch verwertbaren Daten mehr da sind. Wir haben es auch erlebt, dass Man-in-the-Middle-Schaden erst ein halbes Jahr später gemeldet wurden. Dann muss ich keine IT-Forensiker mehr haben. Die Daten sind weg. Da gibt es keine Log-Dateien mehr. Dann brauch ich IT-Forensiker nicht mehr.

Dr. Tatia Bagauri: – Wenn festgestellt wird, dass es sich um einen IT- oder Cybervorfall handelt, müssen weitere Schäden verhindert werden. Worauf sollte Ihrer Erfahrung nach in der Praxis besonders geachtet werden?

Jan-Henning Evers: – Natürlich, wenn ich einen Incident habe, (z. B. die unbefugte Nutzung von IT-Systemen) dann habe ich jemanden, der das macht, was er nicht machen soll. Wenn ich jemanden habe, der etwas macht, was er nicht machen soll, dann will ich, dass er damit aufhört. Das heißt, wenn ich eine Handlung habe, die Auswirkungen oder auch das Ergebnis schon sehe (im schlimmsten Fall eine Verschlüsselung von Daten), dann muss ich es zuerst unterbinden / stoppen. Dafür gibt es unterschiedliche Maßnahmen. Ich kann es aktiv bekämpfen, z. B. beim Ransomware-Angriff, wenn die Daten verschlüsselt sind, kann ich die Internetverbindung mit allen Endgeräten unterbrechen. Es ist aber nur die Ultima Ratio. Es ist natürlich immer als allererstes in jedem Schadenereignis so. Es gilt nicht nur für Cyber, sondern auch für analoge Ereignisse. Wenn bei mir im Keller der Wasserrohrbruch ist, will ich, dass man das Wasser abstellt und es nicht mehr reinläuft. Das ist beim IT und Cyber-Incident genauso. Wenn jemand dort wohl sein Unwesen treibt, dann möchte ich, dass er damit aufhört.

Das Nächste, was ich mache, ist es, dass ich weitere weitergehende Folgen verhindere, beispielsweise, indem ich nicht nur die Internetverbindung kappe zu meinem Server, sondern alle Endgeräte abstelle, weil wenn sie weiter online sind und betroffen sind, dann funken sie mit Dritten und könnten den Schadcode weitertragen (die Infizierung).

Dann komme ich sehr schnell zu organisatorischen Maßnahmen, dass ich z. B. alle User auffordere, ihre Passwörter zu ändern, um Systeme zu härten und eine weitere Verbreitung zu verhindern. Ich schaue immer, dass ich sofort erstmal diesen negativen Einfluss stoppe, dass ich ihn eindämme und es einfach nicht mehr weiter geht. Wenn Ruhe ist / wenn Schluss ist, dann kann ich mir anschauen, wie ich das Problem dauerhaft beseitige und eine Lösung finde.

Dr. Tatia Bagauri: – Sollen die beschädigten Daten aufbewahrt werden, damit sie später als Beweismittel verwendet werden können?

Jan-Henning Evers: – Meines Erachtens sollen die Daten nicht aufbewahrt werden. Sie müssen forensisch gesichert werden. Das kann man machen, indem man davon Images macht. Damit ist es rechtlich sauber. Die Daten werden also bei den Forensikern kopiert. Images werden mit entsprechenden Forensik-Tools gezogen und es reicht m. E. vollkommen aus. Die Festplatte muss nicht aufbewahrt werden.

Dr. Tatia Bagauri: – Gibt es etwas, das im Falle einer Datenschutzverletzung auf jeden Fall gemacht werden sollte, was man im Fall eine Informationssicherheitsvorfall nicht machen würde?

Jan-Henning Evers: – Nein, gar nichts! Die Sicherung der forensischen Beweise erfolgt ganz am Anfang. Die Bewertung, ob es ein Informationssicherheitsvorfall oder / und eine Datenschutzverletzung ist, erfolgt viel später. Ich kann es vorher nicht entscheiden. Das ist das, was ich am Anfang meinte. Ich muss den Sachverhalt vollumfänglich erfassen, um ihn später bewerten zu können, und dann kann ich bewerten, ob es eine Datenschutz- oder Informationssicherheitsverletzung ist, ob es eine sonstige haftungsrechtliche oder arbeitsrechtliche Komponente hat. Ansonsten klingt es so, als ob Schritt zwei vor dem ersten gemacht wird. Also, zuerst alles sichern, was möglich ist und dann festlegen, was man davon braucht und was es für Auswirkungen haben kann.

Dr. Tatia Bagauri: – Welche Rollen, Abteilungen oder Bereiche müssen unbedingt in den Vorfall einbezogen werden?

Jan-Henning Evers: – Es gibt zwei technische Workstreams: Die IT-Forensiker und IT-Instandsetzung, zwei organisatorische Workstreams: Die Betriebsorganisation und die Betriebsunterbrechung, den Krisenkommunikation-Workstream (inklusive der Erpresser-Kommunikation) durch die interne und externe Kommunikation und vier Legal Workstreams: Datenschutz, die Kommunikation mit der Polizei, sonstige rechtliche Haftungsfragen und die Fragen zur Versicherung. Man braucht alle. Den IT-Forensiker braucht man immer, denn der ermittelt den Sachverhalt. Die anderen kommen dann, wenn sie gebraucht werden. In den großen Schäden / in den Ransomware-Attacken, haben wir alle Workstreams, und sie sind auch besetzt. Es gibt Personen, die mehrere Bereiche abbilden können, d. h. sie können mehrere Workstreams leiten, aber jeder Workstream hat seine eigenständige Berechtigung und muss eigenständig geführt werden. Ob ich ihn brauche, weiß ich erst, wenn ich den Sachverhalt kenne. Ich kann nicht sagen, ich habe eine neue Schadenmeldung erhalten, und ich sage heute, dass es kein Datenschutz-Thema ist. Das weiß ich noch nicht. Das kann ich erst wissen, wenn ich den Sachverhalt analysiert habe. Dann merke ich vielleicht, dass ich doch ein Datenschutz-Thema habe.

Im Allgemeinen kann man diese Bereiche wie folgt einleiten: 1. Technik / „Technology“, 2. Organisation / „Operation“, 3. Kommunikation / „Communication“ und 4. Legal. Diese vier Themenfelder braucht man immer beim Incident Response. Es wird fast keinen Fall geben, wo man nicht alle diese vier Themen benötigt.

Dr. Tatia Bagauri: – Wie wird im besten Fall von einer Organisation nach einem Sicherheitsvorfall die abschließende Überprüfung durchgeführt? Worauf ist Ihrer Erfahrung nach in dieser Phase besonders zu achten?

Jan-Henning Evers: – Man muss ehrlich und offen analysieren, was passiert ist. Wir kommen immer wieder auf die gleichen Punkte zurück. Ich muss mir sehr aufmerksam anschauen, was passiert ist, also den Sachverhalt zusammenfassen und ihn mir erschließen. Ich muss ihn ehrlich und offen bewerten. Wenn ich beispielsweise eine technische Sicherheitslücke habe, dann muss ich diese schließen, ansonsten passiert mir es wieder. Ähnlich ist es, wenn ich beispielsweise den Einbrecher im Haus habe und merke, dass ich keine Tür eingebaut hatte. Ich kann die Polizei holen, und er wird gehen. Wenn ich mich aber wieder ins Bett lege und habe noch keine Tür eingebaut, muss ich damit rechnen, dass er bald wieder kommt. Es ist bei der Technik genauso. Ich muss die technischen Schwachstellen auf der Hard- und Softwareseite (meistens auf der Softwareseite) schließen.

Eine technische Lücke entsteht meistens, weil jemand (es ist typischerweise bei der IT-Sicherheit der Fall,) etwas nicht gemacht hat, z. B. nicht das aktuelle System verwendet oder nicht gepatcht hat. Dann muss ich mir als Unternehmen überlegen, warum es passiert ist. Ich habe vielleicht niemand, der für IT zuständig ist. Ich habe einmal alles gekauft, und seitdem benutzen wir das. Dann muss ich jemanden für die IT- Sicherheit, für IT-Wartung oder IT-Leitung einstellen. Vielleicht habe ich jemanden eingestellt, der das macht; er macht es aber schlecht. Warum? Weil er von mir nicht richtig angewiesen wurde. Dann muss ich dafür Sorge tragen, dass ich als Chef oder als Geschäftsführer, die Aufgaben und Verpflichtung auf den fähigen, gut und sorgfältig ausgesuchten Mitarbeiter übertrage und ihm sage: „Bitte mach das für mich!“ Wenn ich weiß, dass der IT-Leiter vorher Metzger war und er keine Ahnung von IT hat, dann sollte ich mir jemand suchen, der Informatik studiert hat und nehme ihn. Wenn ich den Metzger nehme, dann muss ich mir vorwerfen lassen, dass ich ihn nicht sorgfältig ausgesucht habe. Vielleicht muss ich auch zu der Entscheidung kommen, dass meine IT so komplex ist und ich es extern auslagern möchte. Ich muss die richtige Maßnahme dafür treffen, dass es nicht nochmal passiert.

Man muss ehrlich und offen analysieren und die Sicherheitslücken technisch und organisatorisch schließen. Es kann natürlich so weit gehen, dass man sich von Mitarbeitern trennt, das kann so weit gehen, dass man neue Mitarbeiter einstellt, das kann so weit gehen, dass man Aufgaben insourcet / outsourcet, weil die aktuelle Lösung nicht gut ist. Es kann auch sein, dass der externe Dienstleister schlecht ist und muss man einen neuen beauftragen. Man muss das Geld investieren und dafür sorgen, dass es nicht nochmal passiert. Diese Maßstäbe kann man nur herausfinden, indem man ehrlich analysiert und sich nicht belügt.

Anlage 4 – Interview im Rahmen der Information Technology (IT)

Kyle Duncan

Information Technology Application Manager at COGITANDA Dataprotect AG

Interviewed on 17.02.2023

Dr. Tatia Bagauri: – If a U.S. provider receives a request from a U.S. law enforcement agency for data stored in its EU-based subsidiary that contains information about E.U. individuals, whether or not to release that data depends in part on the organizational structure of the U.S. company. If the U.S. provider has possession, custody, or control of the data sought, that data would have to be released under the CLOUD Act. Is it technically possible to separate processed data in Europe in such a way that it is not accessible to the authorities in the U.S.? What would be the best technical solution to physically and logically separate data from facilities outside of the U.S. and in the U.S. to ensure that it is not in "possession, custody, or control" of the U.S. provider?

Kyle Duncan: – Probably! The answer is: It depends. If you have Company A which is based in Europe and you want to open up a subsidiary in the U.S. for the North American market, Company B, you would need to have (this is where I'm starting to navigate into legal manners which is outside my scope of knowledge) a hierarchical separation where Company B could not demand or have control over the E.U. either citizen or employee data. So, you would need to have any data that you don't want shared with the U.S. government siloed entirely in the E.U. with no possible way of accessing it from the U.S.

From a technical standpoint, that is certainly possible to be done. It's just a matter of having whatever servers you're utilizing located in the European Union. If you want to be extra sure, you would want to have a B part of a cloud solution that is only U.S. based, so not in an AWS or deployment.

Dr. Tatia Bagauri: – In this scenario that you've just mentioned, how possible is it to have it as a regular standard? Or can I even go deeper and say that for a particular project, I can have one kind of access restriction and for another customer or project another one? How practical is it to implement it in daily business?

Kyle Duncan: – Ultimately, and this will be a repeated answer throughout the rest of the questions: Security depends entirely on access! If you are opening up another company in the U.S., presumably your services are similar or the same and thus the data that you're acquiring and using is going to be similar or same. If you are not able to segment your company so that data cannot be completely separated, you then need to look into means of anonymizing it to a degree where it is legally considered to be GDPR compliant. The question, if it is possible, entirely depends on what your business is. You can always have, as I said before, your data silos separate by region and have an IT team that is separate from your North American based one and your European based one. You're going to end up with duplicated hierarchies, because you can't have one reporting to the other. Overall, the question is more of a legal question than a technical question.

Dr. Tatia Bagauri: – In cases where critical / sensitive data is stored in the cloud, state-of-the-art security, including encryption at rest and in transit, should be used. Direct requests from foreign authorities may be refused in such cases. In any case, the management of the encryption key must be under the full control of the service recipient and must not be accessible to the U.S. cloud service provider without the permission of the person responsible for the data. How useful are these tools and actions against the requests of foreign authorities? How much time and material effort would it be for an organization to implement them? Will this solution work for the data that is not stored in the cloud?

Kyle Duncan: – Let's approach this from the technical portion first. You've already touched on some of the challenges. Encryption at rest and in transit is just a standard that is for you to be considered even remotely secure. That is just a requirement. There are different algorithms for encrypting and decrypting data. I can't advise what is the best way to do it, beyond that you will be looking to asymmetrically encrypt the data store. You must be sure that it is a sufficient enough encryption that it can't be brute forced. The key that's used to decrypt, should be stored in an air gapped location so it shouldn't be something that's accessible from a network attack and that key, as you mentioned, should not be accessible to whatever cloud service.

Let’s say that I am the CTO of a company in Europe. I should not have access to the key to decrypt the data store and, in fact, that key should essentially be used through programmatic means to create session tokens that are used to decrypt certain portions defined with a definable scope. A foreign authority contacts me and says: “You need to give us all of your data because the XYZ law has been breached. You have 30 days to comply.” At this point, it's a lawyer thing.

Ultimately, people are your weakest point of security. So, you need to keep people separate from the actual secrets. If I'm scooped up by the police, and they say: “Give me all your passwords!” I will give them all my passwords. That's just how it's going to be. If I don't know that information, I can't give it. That's where we've reached the limit of technology and are going into law.

How will this solution work on data that's not in a cloud? It's the same sort of process. Let's look at a cloud first and then we'll talk about a self-hosted scenario. Any cloud service provider or any major service provider has an agreement that you enter with them in order to use their services. We'll use Azure or AWS as an example. They are service providers, so they are responsible for the infrastructure itself, how you interact with it, how you transfer data to them and how they secure that data. They are responsible for the data being encrypted in transit and at rest. The data itself is your responsibility.

Making sure that you have the proper encryption in place (you can also set your own keys or you can use theirs) is also something you need to be mindful of with the self-hosted option. The other thing is that you need to be aware that in order to be truly secure with data you need to have multiple copies that are also secured and are in separate and independent locations. If we talk about the self-hosted option, then you are essentially taking that service provider role onto yourself. Instead of having a corporation, such as Microsoft or Amazon, ensure that your data is secured while in transit and at rest, you need to make sure that this is the case. You also are then in charge of making sure the backups are being done regularly, that your copies are the redundant copies, and that everything is secured and is following whatever ISO policies require.

Dr. Tatia Bagauri: – How useful do you think it is to use VPN in the organization to protect the data while transferring or at rest?

Kyle Duncan: – The idea of using a VPN is so that your traffic is centralized, so you can track what data is being transmitted for purposes of data loss prevention, and also so that no one else has access to it. The security companies are also using the idea of a zero trust network access which instead of using a VPN can connect to a proxy service and then all traffic is routed through that. It's kind of an offering alongside a data loss prevention program if a company wants to keep their communication centralized.

Dr. Tatia Bagauri: – One of the ways to pseudonymize or anonymize the data is to use complex mathematical formulas (known as “hash functions”). They determine a specific code from the personal data that applies both to a concrete data set and to the person behind it. Could you please describe in more detail how the hash functions would look in practice?

Kyle Duncan: – When you store data, it should be encrypted. We're still following the earlier mentioned encryption at rest and in transit. When we're looking at the decrypted data, you should have essentially key value pairs. It looks like nonsense because we've hashed these functions or these data. What is hashing? Hashing, as you said, is a mathematical function that takes an input and then outputs a string of indeterminate size that cannot be related back to the input, unless it's reverse engineered. So, that's the point of needing the anonymization, particularly for data that has a known size and character restriction. As an American, a social security number would be the usual example. These functions can be reverse engineered. It's as simple as saying, I'm trying to think of a SHA-256 or a ES512 function and just putting in numbers until I get something that matches what you have. In fact, if I'm a hacker and I'm looking to turn this hash into something useful for me, I already have a library of what those values are ahead of time. So, you can just plug in go B025 FC3 that's the letter there that's #7. Because I know now that this is the function you're using. The rest of it, I just have. So, if you only hash your values that's not sufficient. You should also have a replacement for the anonymization, so that even if that data is obtained and unhashed, you can be a bit more confident in the security, because it just results in something that can't be tied to a person.

In summary, the data should be encrypted overall. Once it's decrypted, we then have the hashed values. Those hash values should not be able to point to a given person. Those hashed values should be anonymized, so that even if they are unhashed, then still the person is not affected.

Dr. Tatia Bagauri: – ISO 27001: A.8.9 requires the definition, documentation, implementation, monitoring and review of the (security) configurations of hardware, software, services and networks. In addition, it is important to react to changing conditions, continuously review the configurations and adjust them if necessary. How important is configuration management to the overall security level of an organization? What role can configuration management play in digital data transfer? What in particular needs to be taken into account in configuration management while transferring data?

Kyle Duncan: – Configuration management as a concept is a very broad topic and is usually the reason why you have separate people in a security team dealing with network security, users' security, endpoint security or e-mail security.

What role can configuration management play in digital data transfer? In order for the digital data transfer to be secure, you need to be sure that you're managing all layers. You need to make sure that all layers are secured. If we talk about the data being encrypted in transit, that's already talking about the network layer. These are the actual packets being sent between the server and my machine.

How do we make sure that encryption is going to fulfill its needs? If we look one layer down to the data link, we are talking about the routers in between the ethernet, essentially the actual connection between myself and that server. We need to make sure that there isn't someone who's physically in the way to say: "I observed your exchange and now I just have all your data". If we look above that, we can think about the actual application. This is a few layers above. Your encryption in transit doesn't really matter if you have someone who has remote access to your workstation and is just looking at everything that you're doing and recording. You can encrypt as much as you want; it doesn't actually matter. At the same network level, you should be utilizing some means of encrypted traffic in a safe VPN connection, IPsec, or IKE. At each of these levels, there's essentially a means for someone to defeat your security measures and gain access to things that you don't want them to have access to.

Dr. Tatia Bagauri: – From your perspective, as an IT, when is it easier to work: When you have something written before, let's say a guideline, or would you say this makes life harder? Especially when it comes to management, I think it's necessary for roles, responsibilities or steps to be written down before implementation. However, this is from my perspective as a person who is writing or planning. What would you say from the perspective of a person who is actually implementing? Would you say it makes your job even harder or slower or would you say it helps?

Kyle Duncan: – It is entirely a matter of perspective, in the sense of how comprehensive ISO 27001 is. Does it make my life harder? There's a lot to manage and take care of and what not. However, if you just try and go off, you're on your own. You can try and make things secure, but it's probably not going to work well. In the sense of making my life easier: Security is one of the first things that can be forgotten or overlooked, particularly when creating a new company. It's also difficult for me to imagine a world where it doesn't exist.

Dr. Tatia Bagauri: – To prevent data leakage, data should be identified as well as classified, and existing communication channels should be monitored. Data leakage prevention tools, monitoring communication behavior and reporting suspicious activities or blocking their transfer could also be used. How practical and effective are these measures? How can they be implemented in practice? What in particular should be taken into account? Are there any other measures that also should be taken into consideration to prevent data leaks?

Kyle Duncan: – Data loss prevention constitutes essentially two parts and you touched on this in your explanation. It primarily boils down to identification of resources and tracking of those resources. Identification is typically done with either checksums or digital signatures of files that are deemed to be important. When we are tracking a file being moved around, we don't want to say: “Oh, here's confidential file A and all of its contents. Check to make sure that none of this ends up anywhere.” Essentially, then it's already leaked.

A checksum is another hashing function that takes the input and then you have something you can check it against. Of course, then you run into the issue that you mentioned before where if you are hashing something, you need to make sure that it can't be unhashed. In other words, where you can get into digital signatures which use asymmetrical encryption to make sure that the checksums like the output is only reachable, if you have the appropriate key. It works similarly to IPSec where you have an additional key transfer and / or initial public key transfer. If the recipient has the private key, then he should be able to decrypt the data he is in, and then that data should only be a hash. So, you're not actually obtaining the file itself. You're just naming the file. That's the identification.

The tracking is monitoring internet traffic primarily to see if this confidential file is on an end user's computer. This is an issue 1. if they should not have it, and 2. if they try to send it somewhere. For this reason, DLP is actually largely focused around accidental leakage. There's the concept in particular of shadow IT, which is people who spin up web services or install software that IT is not aware of and, in doing so, accidentally create additional attack vectors in the various actors. DLP is largely focused on trying to prevent those things because the unfortunate truth is, if there's someone who is looking to sell company secrets and they get access to a file and they look at it, they can just take a picture of it with their phone. There's nothing that you can do to prevent that. However, and the key thing here is, if you can track the file which was sent to that individual and then create a trail, then you can use that in your court case that's going to be coming up. So, the question of, do I find it a proper approach? Absolutely!

How can it be implemented in practice? It’s a large undertaking. I mentioned the Zero-Trust Network Access and VPN. Your organization should have means of tracking communications across networks that network transfer. Anything that is very confidential or protected should only be accessible across those modes of transportation. If you have public access to a trusted source, then you may never know if someone is accessing it without your knowledge.

Securing means of access: As I mentioned before, with endpoint security you should know what is on your employees’ workstations. If they have something that they need for their job function, that’s great. But if they get access to something they should not, then you can have a talk with them and say: “You accessed this file. Why are you doing this?” I would say, nine times out of ten, they would say either “I had no idea.” or “I saw it and I opened it.” You can then have a conversation of, “Just because you have access to something doesn't mean that you should look at it”. In one of 10 cases, they don't say anything and / or admit to trying to do something not good.
Measures that should be taken into consideration to prevent data leaks are largely to restrict access. The more confidential something is, the less avenues of access there should be.

Dr. Tatia Bagauri: – So, it is, as you mentioned, a better approach if you have DLP as a project and not just taking care of some particular issues around this topic, right?

Kyle Duncan: – Yes, linking together is incredibly important. By having multiple layers of protection, you make it less likely for something to occur. If we refer to the earlier question with this internalization and on an anonymization: For example, a file was leaked, and we didn't notice it. Our DLP failed. This is already an issue. The hacker needs to have the means of decrypting the data. Well, they did. It was hashed. It's not actually the data there. They were able to reverse engineer it, and now it's dehashed. The data was anonymized, so they didn't actually get anything useful. They got some figures about our customers, but they don't know who the customers are. Lastly, they actually have our customer list, due to something unrelated. There's five different means that they have to have access to before we get into trouble. Linking these together, having a holistic overview, and having a standard configuration across all services, is the best way of protecting your organization.

Dr. Tatia Bagauri: – As you described, access is quite a powerful tool which an organization really needs to take care of to prevent its data being breached.

Kyle Duncan: – Yes, it is. To that point, look up zero trust policies. This is the way that securities moved, I'd say, within the last five years and is continuing to move forward towards the idea that you should never trust that an actor is who they say they are, unless absolutely necessary and you should have the least amount of rights (that's another term and concept) applied to a given operation. This is something that is applied to people but also to automated processes. Let’s say, we're backing up site A's data but that site A's data needs to go to backup location C. The process that implements it, should only have the ability to read the data of site A and only be able to write the backup at location C and it should only have it for the window of time in which this operation needs to take place. Any other time, it shouldn't be able to do anything. This is the concept of least amount of rights / “Principle of Least Privilege”.

We also need a means of authenticating that this backup process is actually the process that we're expecting. Usually that's done with session token. So, you can generate a token that can be used for a certain amount of time and afterwards it's no longer valid. These are the ways that we can limit access in a way that allows users and processes to do the jobs they need to, but in a way that's controlled, manageable and trackable.

Dr. Tatia Bagauri: – You already mentioned backups and this is quite a huge topic. Backups are a very useful tool. According to ISO 27001: A.8.13, backups of information, software as well as systems shall be addressed in a policy and shall be tested regularly. What type of backups are the most efficient to create? Are cloud backups a good idea or should it be avoided? Is it ok to keep backups encrypted on the server?

Kyle Duncan: – We have the rule of thumb out saga in IT, one is none. So, if you make one backup of something, you're still at a single point of failure. Typically, you have three backups. Historically, you would have a local backup. So, if something happened in your production environment, then you just need to get your live backup, that's right there, and you can hopefully get back up and running within a few hours. Then, you have a secondary off-site backup. That is usually something that is backed up, let's say, weekly and values I give are entirely dependent on what is necessary. Let's say, we bring the hard drives or media to an off-site location once a week, and then every month, three months, six months. You have a third location where you bring backups.

The idea here is, how valuable your backup is, where is it located, and how many copies you have overall. Data should be backed up to different areas and be accessible in different ways. While storage is getting cheaper every day, it is still expensive if you're looking at an international company with terabytes of data or hundreds of terabytes or petabytes. Something that is on demand available, ready to go, gets incredibly expensive very quickly. Historically, tape is your backup medium. It is slower to access, however, you can store a lot of information on tape and then have it be serviceable for several years.

What a lot of companies use now is cloud storage because managing server firms and backup locations manually is a time and monetary expense. You need someone to administrate these backups which you will also need in a cloud situation. However, you will need a lot more staff in order to do it yourself versus a cloud backup. The cloud infrastructure is handled for you. You just need to supply the configuration requirements.

In general, a cloud backup is not less secure than renting Rackspace in a data center because most companies would not build their own data center if that's an expenditure. The use case of going for cloud is typically that the company is small and either does not have the funds or manpower in order to manage its backups itself. You can use one of these services or do a hybrid approach, where you have something on premises and then you back it up to an AWS service or one of these companies. That way you have the best of both worlds.

Is it Okay to keep backups encrypted on the server? I hope you keep them encrypted! If they are not encrypted, then you've just defeated your entire security policy. I think this question is more about if it's fine that backups exist somewhere encrypted. The general answer is the same as one of your previous questions where only the person responsible for storing data in the cloud should be the only one who has access to the key. It is standard practice that whichever cloud provider you use, the provider doesn't have access to your data, because they don't have access to the keys.

To have data that is not encrypted, is not secure. There is a legitimate concern in terms of encrypting data; so if you lose the key then you don't have access to it anymore. That's just a risk you have to take as part of a Security Administration and you need to make sure that your keys are secured, which means that you have a backup plan in case it goes down, you need to have a means of backing that up. There's no primary reason for not encrypting, unless it's some legacy software that just cannot handle it. Then you need to figure out a way to restrict access as much as possible.

Dr. Tatia Bagauri: – So, this would be the same explanation if I say that I do not use passwords for my applications because I may forget or lose them.

Kyle Duncan: – Yes, that's a very good allegory.

Dr. Tatia Bagauri: – In your opinion, what would be the best instrument / measure / tool to ensure international data transfer that is legally compliant and technically secure?

Kyle Duncan: – I've never had to deal with managing a project that had to transfer data internationally outside of well established processes with that disclaimer either way. If I was given this task, I would approach it with the mindset that we have our local data store in the European area. We have, let's say, the U.S. area and we want to have a data silo in the middle. The reason for this is to transfer data internationally in such a way that you're not exposing the entirety of your E.U. company to the U.S. side, you need to restrict access. At least in my mind, I would want to have a data silo in between. This might be a SharePoint, a server, a database, or something in the middle. If it's something hosted by companies such as SharePoint, OneDrive, or Google Drive, you have a data processing agreement with them and that restricts what data can go from you to them, legally what essentially they're responsible for through the GDPR.

On the E.U. side, you have a data loss prevention policy in place that tracks what data is actually being given. The means of access to your network transport layers should be using a VPN or zero trust network access following along those lines, so that you're limiting the traffic between you and that silo. That also enables you to track what is actually being sent there. From an application point of view, you should limit who is able to send this data. The idea here is that we're trying to prevent the government or foreign authorities from being able to say: “You need to give us more stuff because XYZ”. In this scenario, I actually shouldn’t even be part of the project because I’m a U.S. citizen. The U.S. government has a little bit more over me than it does an E.U. citizen. Ideally, I shouldn’t even know that this exists. (That’s actually beyond application. That’s more a personnel legal portion.)

So, only certain people should have access to be able to send it. It should be sent securely with the VPN and ideally the application has only certain people who can send. That's how we're getting from the E.U. to the silo.

From the U.S. side, it's kind of the same thing in reverse. Only certain people should be able to retrieve data from that service. Those people will likely be U.S. citizens. I don't think you can transplant E.U. citizens just to try and accommodate this and even so, they're operating on U.S. soil, so any legal restrictions go up the window.

From an application point of view, only certain people should have access. The access should be done over a secure channel because if you are limiting it, but then a man in the middle is able to decipher it, then everything is destroyed. Ideally, the silo is in the E.U. and enters into a Data Protection Agreement with the U.S. based company. So that you have an agreement with the silo and the E.U. company and the silo and the U.S. company, there must be a clear line of communication between them and then from there you should be protected ideally from a legal and technical point of view. This also means that, if anyone leaves the company or anyone is restricted further, it's sort of a separate entity from your day-to-day activities in either company.
GDPR is a complex topic. International relations and what you realistically can do against a nation or nation state, is also very much a complex topic. However, if you are taking into consideration means of access, who can access and how you are monitoring and recording this, that is to say recording in the ISO certification and standard operating procedures, you're covering all your bases.

Dr. Tatia Bagauri: – What would you say from the perspective of you as a technical staff, would you say GDPR makes life harder or the American legislation is tailored too easy? Let’s say, you are the boss in the U.S. company and the boss in the European company, what would you say: Is it too tough to implement European legislation or is it too easy to implement American legislation?

Kyle Duncan: – I think, no one fully understands how much impact data has, particularly as AI is making leaps and bounds. Working with GDPR is a nightmare. It is a very difficult process and set of rules and that's simply because so much data is generated. As we go on, it increases exponentially. To be able to accommodate all of that data requires a very strict set of rules. So, overall I think it's absolutely necessary. I was not happy that the CLOUD act passed back in 2018. Concerning the administration at the time, it was always going to pass. I blame the administration at the time, but frankly we had the PATRIOT Act passed in 2001, so the 4th amendment doesn't mean anything.

In summary, GDPR is absolutely necessary. As it moves forward, it is going to need to become more strict, because people are made of data, whether they want to be or not and if that's not protected, then people are not protected. That's kind of blending the technical point of view and my personal point of view. Luckily, we are also seeing legislature coming out of California. That is centrally doing something similar if not the same thing as GDPR. What California does the rest of the country follows. Overall, we should be moving towards the idea that data should be protected by default and not as the afterthought.