Alinto

White paper

November 2022

DIGITALE SOUVERÄNITÄT: WELCHE HERAUSFORDERUNGEN FÜR BUSINESS E-MAIL?

Inhalt

Einleitung

Die digitale Souveränität steht heute mehr denn je im Mittelpunkt der Aufmerksamkeit der Unternehmen. **Sie wirft Fragen zum Datenschutz, zur Vertraulichkeit und zur Unabhängigkeit der Unternehmen von amerikanischen Lieferanten (insbesondere GAFAM) auf**.

Es ist eine zentrale Frage, die sich auch angesichts der aktuellen geopolitischen Lage stellt (Krieg in der Ukraine, Krise in Taiwan usw.), in der die meisten Cyberangriffe von autoritären Staaten wie Russland oder China ausgehen (laut dem Bericht von Carbon Black1). Europäische Unternehmen müssen ihre Daten zuverlässig schützen und sich verstärkt auf ihre Souveränität konzentrieren.

Open-Source-Technologien bieten einige Lösungsansätze. Die Transparenz der Software ermöglicht den Unternehmen einen Einblick in die Funktionsweise der Anwendungen und die Speicher- und Verwendungsarten der Daten. Hinzu kommen zahlreiche nationale und europäische Initiativen, die die Branchenriesen auf den Prüfstand stellen:

Vorschriften (DSGVO), das Bewusstsein für Souveränität und die Verbreitung von Open-Source-Technologien ...

Auch geschäftliche E-Mails sind betroffen. Diese sind regelmäßig Cyberangriffen ausgesetzt und machen sie deshalb zu einem vorrangigen Ziel der Sicherheitsmaßnahmen. Dabei bleibt ihr operationeller Betrieb in Bezug auf die Weiterleitung und Speicherung von Daten kompliziert. In diesem Whitepaper werden die digitale Souveränität, die europäischen Initiativen in diesem Zusammenhang und das Potenzial von Open Source für die Sicherheit aus dem Blickwinkel der professionellen Business-E-Mail-Lösungen unter die Lupe genommen.

[1] https://www.developpez.com/actu/216086/La-Russie-et-la-Chine-sont-les-deux-principales-origines-des-cyberattaques-dans-le-monde-entier-d-apres-un-rapport-de-Carbon-Black/

Digitale Souveränität als Herausforderung

Debatten zur digitalen Souveränität stehen heute im Mittelpunkt der digitalen Strategien der Unternehmen. Souveränität ist nicht nur ein protektionistisches Schlagwort, um den digitalen Rückstand Europas zu kompensieren. Sie zielt darauf ab, den **wirtschaftlichen Erfolg und die Unabhängigkeit von Unternehmen durch den Schutz ihrer Daten, Kunden und Mitbürger zu gewährleisten**.

Die Wahl einer souveränen digitalen Lösung ermöglicht es Unternehmen, sich drei großen Herausforderungen zu stellen. Hier sind einige Erläuterungen.

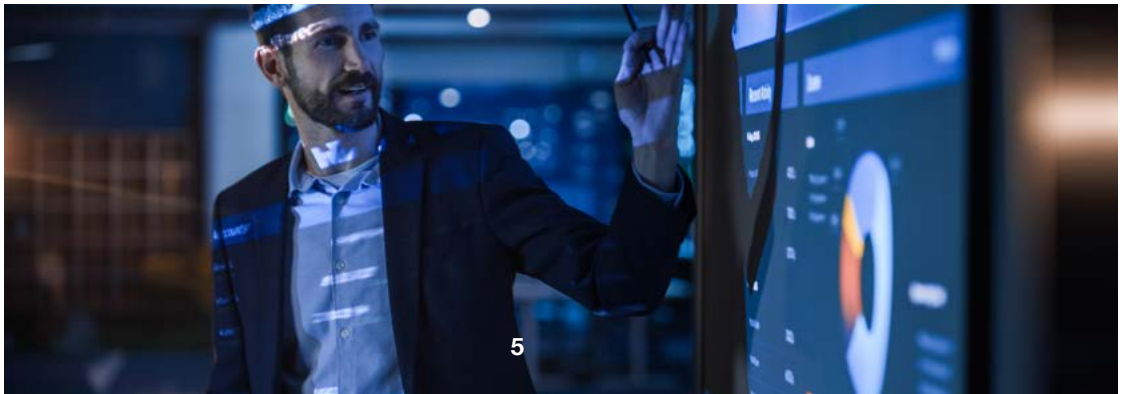
Souveränität, um die Kontrolle über die Daten zu behalten

Das Thema Datenschutz steht aktuell bei den meisten Unternehmen auf der Tagesordnung. Seit dem Inkrafttreten der DSGVO im Jahr 2018 hat sich das Bewusstsein für den Schutz personenbezogener Daten in Europa deutlich verbessert. Aber nicht alle Länder und Gesetzgebungen gewährleisten den gleichen Datenschutz. Es ist daher von grundlegender Bedeutung, **diese Daten zu erfassen und sicherzustellen, dass sie geschützt und für unbefugte Personen nicht zugänglich sind**.

Unternehmen können verschiedene Maßnahmen ergreifen, um ihre Daten zu schützen.

- Nutzen Sie für Ihre Daten eine **souveräne Cloud**, die sich in Europa befindet und von Unternehmen betrieben wird, die europäischem Recht unterliegen. Dies kann durch verschiedene Gütesiegel, wie beispielsweise SecNumCloud, eine der anspruchsvollsten Zertifizierungen für das Hosting in Frankreich, garantiert werden.
- Entscheiden Sie sich für **Open-Source-Software** und/oder europäische Software.
- Stellen Sie sicher, dass Ihre Mitarbeiter die verschiedenen rechtlichen **Datenschutzbestimmungen** kennen.
- **Sensibilisieren Sie Ihre Mitarbeiter** für die Notwendigkeit eines angemessenen Datenmanagements.

Souveränes Hosting schützt Ihre Daten auch rechtlich vor unerwünschten Zugriffen. Es ist die Basis einer guten Datenkontrollstrategie für Unternehmen, die einen Mehrwert aus ihren Daten ziehen und gleichzeitig die Vertraulichkeit für ihre Kunden sicherstellen wollen.



Souveränität als Antwort auf den Cloud-Act

Der Cloud Act ist in den Vereinigten Staaten seit 2018 in Kraft. Der Cloud-Act ermöglicht es US-Behörden, von Anbietern von Kommunikationsdiensten, die dem US-Recht unterliegen, die Herausgabe von Daten zu verlangen, die sich in ihrem Besitz, ihrer Obhut oder unter ihrer Kontrolle befinden, **unabhängig vom Standort der Daten**. Dies stellt eine ernsthafte Bedrohung für die Daten europäischer Unternehmen dar, die von US-Anbietern gehostet werden, auch in Rechenzentren mit Sitz in Europa. Gemäß dem Cloud-Act können diese Anbieter Daten, sogar vertrauliche Daten, über den ursprünglich vorgesehenen Verwendungszweck hinaus nutzen.

Die digitale Souveränität Europas zielt darauf ab, **Schutzvorkehrungen gegen den unrechtmäßigen Zugriff durch bestimmte Länder zu treffen**, Zugriffsanfragen ausländischer Behörden zu regeln und die Weitergabe nicht personenbezogener Daten zu verhindern.

In diesem Zusammenhang werden in Kürze zwei europäische Verordnungen in Kraft treten:

- **Der Daten-Governance-Act** wurde im Mai 2022 verabschiedet und tritt im September 2023 in Kraft. Die Verordnung soll die gemeinsame Nutzung personenbezogener und nicht personenbezogener Daten durch die Einführung von Datenaustauschmodellen erleichtern.

- **Der Data Act** (auch Datengesetz genannt) wurde im Februar 2022 vorgelegt und soll die faire Verteilung des Wertes aus der Nutzung personenbezogener und nicht personenbezogener Daten zwischen den Akteuren der Datenwirtschaft sicherstellen, insbesondere in Bezug auf die Nutzung von vernetzten Objekten und der Entwicklung des Internets der Dinge (IoT).

Souveränität als Gegengewicht zur GAFAM-Allmacht

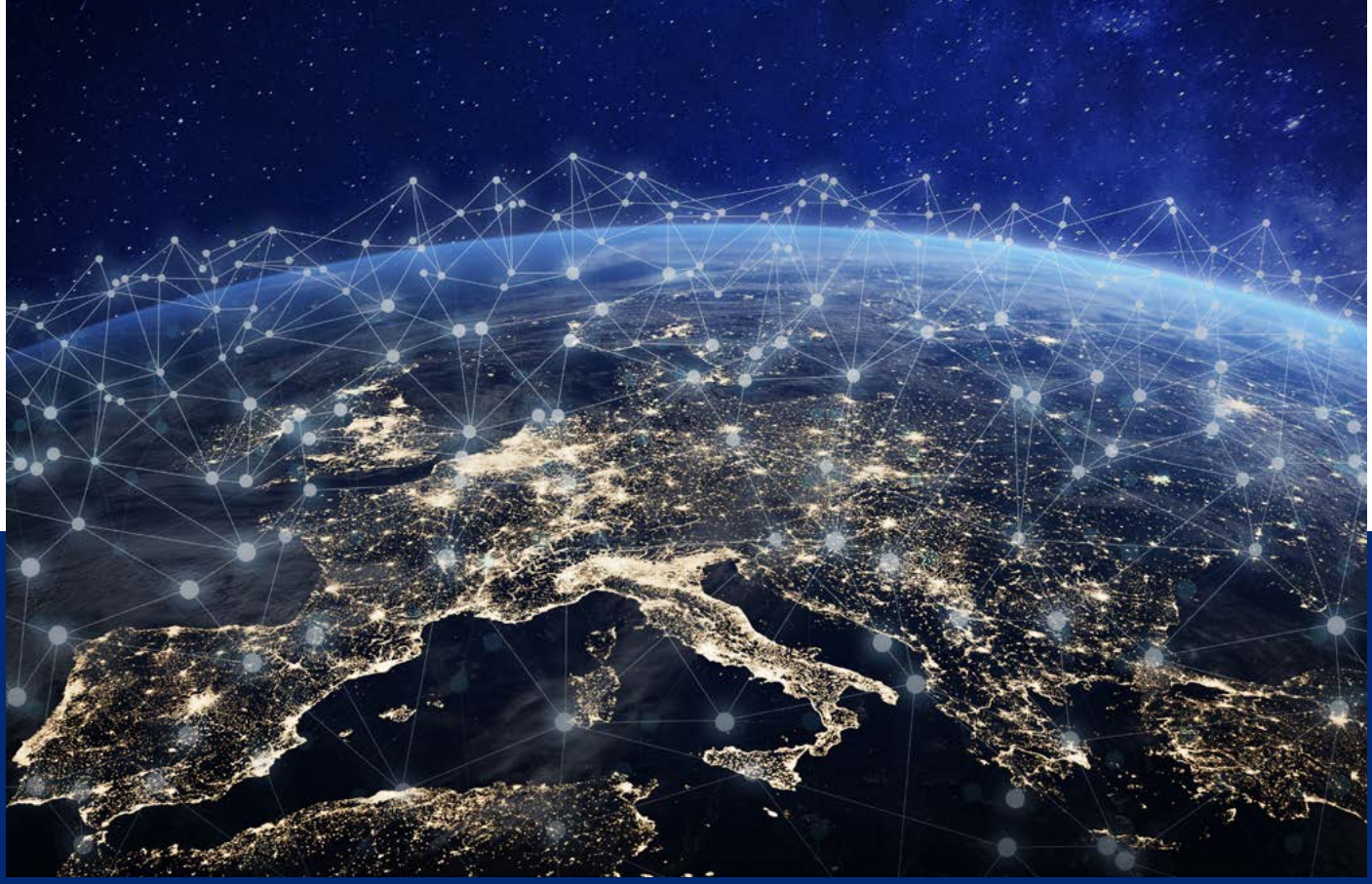
Die GAFAM[1] bedrohen die digitale Souveränität. Die amerikanischen Digital-Giganten haben ein beträchtliches wirtschaftliches Gewicht: «Die Börsenbewertungen der GAFAM erreichten im Jahr 2020 einen Wert von 5.853 Milliarden Dollar. Das entspricht dem Bruttoinlandsprodukt von Japan, der drittgrößten Volkswirtschaft der Welt»[2].

Die digitale Vormachtstellung ist nicht nur wirtschaftlicher Natur, sondern beruht auch auf digitaler Abhängigkeit. Diese Unternehmen verarbeiten und speichern die Daten von Bürgern und Unternehmen aus der ganzen Welt in Rechenzentren, Messaging-Systemen und Clouds, die ihnen bei der Nutzung von Diensten oder Anwendungen mehr oder weniger bewusst «übertragen» werden. Hinzu kommt, dass die GAFAM der amerikanischen Gesetzgebung und daher dem Cloud-Act unterliegen. Dieser erlaubt es ihnen, Daten, die in ihrem Besitz sind, an Dritte zu übermitteln.

Es ist wichtig, dass die übrige Welt, vor allem Europa, dieser Macht durch die Schaffung eines wirklich souveränen Ökosystems entgegenwirkt. Wie? Indem wir die Vorschriften zu diesem Thema anpassen, die Verwendung von Open-Source-Software fördern und offen über die Herausforderungen der digitalen Souveränität diskutieren.

[1] Google, Amazon, Facebook, Apple, Microsoft

[2] https://fr.countryeconomy.com/gouvernement/pib



Digitale Souveränität: Europäische Initiativen

Um die digitale Souveränität Europas zu gewährleisten, ist es notwendig, die Nutzung, Speicherung und Erhebung von Daten zu regulieren. Die dafür notwendigen Datenschutzmaßnahmen sorgen weiterhin für heftige Diskussionen unter den Mitgliedsländern. Dies hat die EU jedoch nicht davon abgehalten, mehrere Initiativen zu ergreifen. Wir möchten uns mit einigen dieser Initiativen näher befassen.

Die allgemeine Datenschutzverordnung (DSGVO): der Ausgangspunkt

Der erste Schritt in Richtung digitaler Souveränität ist die im Mai 2018 in Kraft getretene Datenschutz-Grundverordnung (DSGVO). Sie regelt den Zugang, die Speicherung und die Verwendung von personenbezogenen Daten der europäischen Bürger. Unternehmen, die über solche Daten verfügen, müssen mehrere Anforderungen erfüllen (Löschung von Daten, Konsultation auf Anfrage, Bestellung eines Datenschutzbeauftragten ...). In derselben Verordnung ist festgelegt, dass personenbezogene Daten aus der EU nur in Länder übermittelt werden dürfen, die einen ähnlichen Schutz bieten und die die EU für “angemessen” hält[1].

Die US-Gesetzgebung ist jedoch weit weniger streng als die DSGVO. Der Cloud-Act ermöglicht es der US-Regierung, auf Daten zuzugreifen, die sich im Besitz von US-Unternehmen befinden. Zudem betrachtet man in den Vereinigten Staaten Daten als einen Vermögenswert, der gehandelt werden kann. **Trotz dieser Unterschiede vertrauen viele europäische Unternehmen ihre Daten großen amerikanischen Digitaldienstleistern an, insbesondere für das Hosting**. Dies hat die EU veranlasst, weitere Maßnahmen zur Regulierung des Datenmarktes zu ergreifen.

[1] Consultar https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Daten-Governance-Rechtsakt und der Data Act: Ein Schritt weiter in die Zukunft

Diese beiden Verordnungen ergänzen die DSGVO. Sie zielen darauf ab, einen einheitlichen Markt für Daten zu schaffen, der den Zugang, die gemeinsame Nutzung und die Weiterverwendung von Daten im Einklang mit den Werten der EU unterstützt.

Das Daten-Governance-Gesetz tritt im September 2023 in Kraft. Diese Maßnahme soll die gemeinsame Nutzung von personenbezogenen und nicht personenbezogenen Daten durch die Einrichtung von Vermittlungsstrukturen fördern. Die letzteren werden die Bedingungen für die Weiterverwendung von Daten im Besitz des öffentlichen Dienstes klar definieren und so mit internationalen Marktteilnehmern unter gleichen Bedingungen konkurrieren können.

Ziel des Data-Acts ist es, einheitliche Regeln für den Zugang zu Daten, die von vernetzten Objekten und den damit verbundenen Diensten erzeugt werden, festzulegen. Durch diese Maßnahme soll der Zugang, die Verwaltung und die gemeinsame Nutzung dieser Daten erleichtert werden.

Die NIS2 Richtlinie: Souveränität und Cyber-Sicherheit

Die EU-Richtlinie NIS 2 über die Sicherheit von Netzen im Internet (Netzwerk- und Informationssicherheit) zielt darauf ab, das Cyber-Risikomanagement von Unternehmen und Organisationen zu verbessern. Sie führt zu neuen Verpflichtungen wie Sicherheitsmaßnahmen, Überwachungsregeln und die Verpflichtung, jeden Angriff an nationale Cybersicherheitsbehörden zu melden (z. B. ANSSI in Frankreich)

Jeder Mitgliedstaat kann auf Basis einer Risikoanalyse eine Liste der Organisationen erstellen, die unter diese Richtlinie fallen. Es wird erwartet, dass mehrere tausend Einrichtungen, die mit digitalen Diensten, der Raumfahrtindustrie oder der Forschung zu tun haben, unter die Richtlinie fallen werden.

CNIL und ANSSI: Ein Beispiel, wie lokale Behörden die Einhaltung der Vorschriften in Frankreich sicherstellen

In Frankreich gibt es zwei Einrichtungen, die für die Überwachung der Datenschutzbestimmungen zuständig sind und Unternehmen und Bürgern bei der Abwehr von Cyberbedrohungen Hilfestellung leisten.

Die nationale Kommission für Informationstechnologie und bürgerliche Freiheiten (CNIL) ist eine Regierungsbehörde, die für die Regulierung personenbezogener Daten zuständig ist. Sie hat mehrere Aufgaben:

- **Information und Schutz der Rechte**: Sie beantwortet Anfragen von Unternehmen und Privatpersonen zum Thema Datenschutz. Sie nimmt auch deren Beschwerden entgegen.
- **Unterstützung bei der Einhaltung der Vorschriften**: Sie bietet eine «Toolbox» an, um Unternehmen bei der Einhaltung der Vorschriften zu unterstützen.
- **Antizipation und Innovation**: Sie unterstützt die Entwicklung von Lösungen zum Schutz der Privatsphäre, berät Unternehmen und fördert eine ethische Diskussion über die Frage, wie mit persönlichen Daten umgegangen werden sollte.
- **Kontrolle und Durchsetzung**: Sie gewährleistet, dass das Gesetz in der Praxis angewandt wird.

Die Nationale Agentur für Informationssicherheit (ANSSI), die französische Agentur für die Sicherheit von Informationssystemen, bietet Organisationen Fachwissen und technische Unterstützung im Bereich der Cybersicherheit. Sie stellt einen Dienst für die Überwachung, Erkennung, Warnung und Reaktion auf Computerangriffe bereit.

Maßnahmen der europäischen Regierungen: wichtige Meinungsbildner

Die Regierungen spielen eine wichtige Rolle auf dem Weg zur digitalen Souveränität. Ihr Handeln beeinflusst die Wahl der technologischen Lösungen. Ihre Entscheidungen tragen dazu bei, das Know-how der digitalen Akteure Europas zu stärken. **Lokale Behörden und Unternehmen werden seit einiger Zeit dazu ermutigt, auf Open-Source-Lösungen oder von europäischen Anbietern produzierte Software zurückzugreifen**.

Die Entwicklung des europäischen digitalen Ökosystems ermöglicht es, eine echte Alternative zu den GAFAM anzubieten und die Kontrolle über die Daten zu behalten.

Die Europäer sind sich der Probleme im Kontext der digitalen Souveränität bewusst. Die Aufmerksamkeit der Bürger ist durch Regelungen wie die DSGVO geweckt worden und die Medien berichten über die Leaks von Gesundheitsdaten oder die Möglichkeiten, die sich durch Gesundheitsdaten ergeben. Die Initiativen der Europäischen Union sind zwar erfreulich, aber nicht ausreichend, um der Macht der amerikanischen Giganten etwas entgegenzusetzen. **Die Vorschriften zeigen jedoch den richtigen Weg zu einem respektvolleren Umgang mit den Daten der Bürger**.

Souveränität und Cybersicherheit: Auf das Engste miteinander verbunden?

Cybersicherheit ist eine Voraussetzung für digitale Souveränität. Besonders in einer Zeit, in der Cyberangriffe zunehmen und raffinierter werden. Die Informationssysteme werden immer komplexer und haben öffentlich-private Schnittstellen und oft durchlässigen Grenzen. Zugleich nimmt der E-Mail-Verkehr ständig zu und bietet so eine Vielzahl an Angriffspunkten für Cyberangriffe.

Wenn es um Datenschutz geht, sind Cybersicherheit und Souveränität untrennbar miteinander verbunden. Hier ist der Grund dafür.

Digitale Souveränität, der erste Schritt in Richtung Datenschutz

Laut dem Artikel „Digitale Souveränität: Europäische Initiativen“ soll die digitale Souveränität dazu beitragen, die Daten der europäischen Organisationen und Bürger effektiver zu schützen. Denn wenn man die Dienstleistungen eines Unternehmens in Anspruch nimmt, das sich selbst als souverän bezeichnet, erwartet man, dass es die Daten nur für die angegebenen Zwecke verwendet und sie nicht weitergibt. Diese Garantie wird selbstverständlich durch die Kontrolle, Speicherung und Verarbeitung der Daten, die Einhaltung der Vorschriften sowie die verwendeten Technologien (souveränes Hosting, Open-Source-Software usw.) gewährleistet.

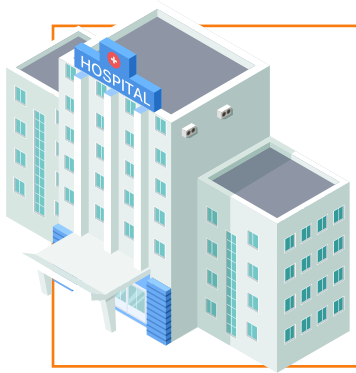
Die Gefahr von Cyberangriffen oder der Offenlegung von Daten kann durch die Zusammenarbeit mit einem europäischen Dienstleister verringert werden

Cybersicherheit: Schutz vor externen Bedrohungen

Der Begriff Cybersicherheit bezeichnet eine Reihe von Maßnahmen, die darauf abzielen, Computersysteme und Daten vor böswilligen Handlungen zu schützen. Cyberangriffe können schwerwiegende Folgen für Unternehmen haben. Unternehmen müssen daher in der Lage sein, solche Vorfälle zu bewältigen, und vorbeugende Maßnahmen zur Sicherung der Informationssysteme einführen.

Zu den Maßnahmen zählen der Einsatz von Sicherheitssoftware wie Antivirenprogramme, Systemaktualisierungspläne (Patches) und Authentifizierungssysteme sowie die Schulung der Mitarbeiter im Bereich Cybersicherheit.

Viele Unternehmen gehen davon aus, dass sie keine sensiblen Daten verarbeiten oder dass ein Angriff nur andere trifft. Die Zahl der Cyberangriffe nimmt aber ständig zu, und die von Cyberkriminellen verwendeten Techniken werden immer ausgefeilter. **Die Folgen können dramatisch sein**.



Ein Krankenhaus in Corbeil-Essonnes (im Süden von Paris) wurde Opfer eines Ransomware-Angriffs, bei dem sensible Daten (PID, persönliche Daten usw.) im Internet[1] veröffentlicht wurden, nachdem das Krankenhaus sich geweigert hatte, Lösegeld zu zahlen.

[1] https://www.liberation.fr/societe/sante/faute-de-rancon-les-donnees-volees-dans-un-hopital-de-lessonne-se-retrouvent-mises-en-ligne-20220925_PMF2MYWN5NAW3BLNDXF7Q34BZY/

Keine Souveränität ohne Cybersicherheit

Digitale Souveränität alleine ist nicht ausreichend, um Daten vor Cyberangriffen zu schützen.

Natürlich ermöglicht die digitale Souveränität eine bessere Kontrolle über die eigenen Daten. Aber Software, die nicht hinreichend geschützt wird, bleibt anfällig für Angriffe. Es ist nicht sinnvoll, digitale Souveränität und Cybersicherheit voneinander getrennt zu betrachten. Es ist wichtig, gute Sicherheitsgewohnheiten in den Unternehmen zu fördern und ein europäisches Cyber-Angebot aufzubauen, das eine echte Alternative zu den Lösungen der amerikanischen Großkonzerne darstellt.

Bis zur Umsetzung eines solchen Systems sollten Unternehmen den Einsatz von Cybersicherheitslösungen nicht vernachlässigen. Das Arsenal umfasst die Verwendung von Antivirenprogrammen, die Einführung von Backup-Strategien, die Unterstützung durch Sicherheitsexperten, die Beachtung von Ratschlägen der Referenzorganisationen (z. B. ANSSI in Frankreich) und das Hinzuziehen von lokalen Fachleuten, die mit Open-Source-Lösungen arbeiten.

Business E-Mails bergen Gefahren!

Die zunehmende Verbreitung von Home-Office, die Einführung von Cloud-Lösungen, die Hybridisierung der IT-Systeme und viele andere Faktoren erhöhen die Gefahr von Cyber-Attacken. **In der Vergangenheit haben Angreifer ihre Angriffe vor allem auf die Infrastruktur von Unternehmen gerichtet. Heute richten sie ihre Angriffe auf Menschen und nutzen deren mangelndes Sicherheitsbewusstsein**. E-Mails sind somit zu einem idealen Ziel für Hackerangriffe geworden.

Demnach stellen auch geschäftliche E-Mails ein Sicherheitsrisiko für den Schutz von Unternehmensdaten dar. Glücklicherweise gibt es souveräne Lösungen, die für mehr Sicherheit sorgen. Hier sind einige Vorschläge.

Business-E-Mail: das häufigste Angriffsziel für Cyberattacken

E-Mails sind ein bevorzugtes Angriffsziel für Cyberattacken, werden doch täglich bis zu 300 Milliarden E-Mails versendet. Über diesen Kommunikationskanal tauschen Unternehmen mehr oder weniger vertrauliche Daten und Informationen aus. Die Perspektiven sind für Cyber-Kriminelle bei diesem Austausch besonders hoch. Das zeigen die Zahlen:

83 % **der Befragten gaben an, dass ihr Unternehmen im Jahr 2021 mindestens einen erfolgreichen E-Mail-Phishing-Angriff erlitten hat.[1]**

Das Versenden von gefälschten Links, das Senden von betrügerischen Anhängen und die Aufforderung zur Eingabe von Bankdaten sind alles Methoden, mit denen die Empfänger einer E-Mail in eine Falle gelockt werden sollen. Ohne eine verstärkte Sensibilisierung der Mitarbeiter und geeignete Instrumente sind Unternehmen dem Risiko von Datenschutzverletzungen ausgesetzt, die schwerwiegende Folgen haben können.

[1] Informe «State of the Phish», 2022

E-Mail und Souveränität: Mission impossible?

Wie kann man Cyberangriffe verhindern? Die Antwort ist nicht so einfach: Die Hacker werden immer raffinierter, und **Nullrisiko gibt es nicht**. Es besteht jedoch die Möglichkeit, das Risiko zu minimieren und den Schutz Ihrer Daten zu verbessern, indem Sie bei der Auswahl eines professionellen E-Mail-Anbieters besondere Sorgfalt walten lassen.

Die von den GAFAM angebotenen Lösungen sind per se nicht souverän. Sie sammeln und speichern Daten in Rechenzentren, die nicht den europäischen Souveränitätsregeln unterliegen. Daher ist es nicht möglich, ihre Vertraulichkeit zu gewährleisten und als Unternehmen die Kontrolle über sie zu behalten. Diese Messaging-Systeme basieren auf proprietären Softwarecodes, die die Abhängigkeit von einem Lieferanten verstärken, ohne dass die Prozesse transparent sind. Dies widerspricht den Grundsätzen der digitalen Souveränität.

Es gibt jedoch Möglichkeiten, die echte Alternativen bieten: Open-Source-E-Mail-Lösungen.

Was macht einen guten professionellen E-Mail-Dienst aus?

Wie sieht die ideale E-Mail-Lösung für Unternehmen aus, die den heutigen Anforderungen an Souveränität und Cybersicherheit gerecht wird?

Die ideale E-Mail-Lösung für Unternehmen ist souverän

Es sollte selbstverständlich sein, dass es sich um eine E-Mail-Lösung von einem europäischen Anbieter handelt, oder aber ein Open-Source-Projekt ist. Letzteres bietet mehr Transparenz über die Funktionsweise und die Bereitschaft einer Gemeinschaft, mögliche Schwachstellen zu beheben. Es gilt aber weitsichtig zu planen. Es ist sinnlos, einen lokalen E-Mail-Partner zu haben, wenn Ihr Hosting-Unternehmen nicht alle Anforderungen an die Souveränität erfüllt.

Das ideale E-Mailsystem besteht daher aus in Europa entwickelter Software, die von einem Dienstleister nach europäischem Recht betrieben wird, der sie auf europäischen Infrastrukturen hostet und nach europäischen Empfehlungen sichert.

Die ideale E-Mail-Lösung für Unternehmen ist sicher

Eine gut durchdachte geschäftliche E-Mail-Lösung umfasst auch ein komplettes Sicherheitspaket. Die in den Standardversionen professioneller Messaging-Systemen integrierten Sicherheitslösungen (Antispam, SMTP-Relay …) sind häufig unzureichend. Viele Unternehmen verabsäumen es, in zusätzliche Sicherheitslösungen zu investieren. **Bis zu dem Tag, an dem sie das Opfer einer Cyber-Attacke werden**.

Ein gutes professionelles E-Mail-System muss daher die besten Technologien an Bord haben, um die Filterung von E-Mails, aber auch die ordnungsgemäße Zustellung von E-Mails zu gewährleisten und gleichzeitig den Ruf der E-Mail-Domäne zu schützen. Dies bieten nur wenige E-Mail-Systeme standardmäßig an.

Um sich wirksam vor Cyberangriffen auf E-Mails zu schützen, sollte das ideale E-Mail-System verschiedene Kriterien erfüllen. An erster Stelle steht ein souveräner Hosting-Partner, dicht gefolgt von einem europäischen E-Mail-Anbieter. Unternehmen, denen die Transparenz des Software-Codes wichtig ist, können noch einen Schritt weiter gehen und eine Open-Source-E-Mail-Lösung wählen. In jedem Fall ist es ratsam, zusätzliche Sicherheitsmaßnahmen zu ergreifen, um ein umfassendes Schutzsystem für das Messaging-System zu schaffen.

Open Source als Schutz für E-Mail-Dienste

E-Mail ist eine unverzichtbare Komponente des täglichen Geschäftslebens. Die Nutzung von Messaging geht weit über die einfache E-Mail-Kommunikation hinaus. Es ist ein effektives und universelles Kommunikationsinstrument, das Zeit spart und viele Kommunikationsvorgänge dematerialisiert.

Es ist unerlässlich, ein effizientes E-Mail-System zu haben, das intuitiv zu bedienen, ergonomisch, zuverlässig und sicher ist. Die GAFAM dominieren den Markt für Messaging-Systeme, die in ihre Office- und Produktivitäts-Suiten integriert sind, wie z.B. Office 365 oder Google Workspace. Es gibt jedoch auch Alternativen. Dazu gehören Open-Source-Messaging-Systeme.

Die Vorteile von Open-Source-E-Mail-Systemen

Ein großer Vorteil von Open-Source-E-Mail-Lösungen ist, dass der Quellcode frei zugänglich ist. Die Nutzung ist unabhängig vom Erwerb einer Lizenz und sie sind **nicht an einen Anbieter gebunden**. Die Einbindung in das IT-System kann intern oder durch einen Dienstleister erfolgen, ohne dass eine Abhängigkeit zu letzterem besteht. Die Transparenz des Software-Codes ermöglicht die Anpassung an individuelle Bedürfnisse zu verringerten Kosten.

Die Nutzer einer Open-Source-Lösung profitieren auch von einer engagierten Community, die die Lösung ständig verbessert und bereichert. In der Open-Source-Community engagieren sich die Autoren für die Weiterentwicklung und Anpassung der Lösung, egal ob es sich um die Ergonomie, Funktionalität oder Sicherheit handelt.

IT-Abteilungen legen einen besonderen Wert auf die technische Nachhaltigkeit. IT-Fachleute **bevorzugen oft die Implementierung von Open-Source-Messaging-Systemen**, weil sie auf ihr Fachwissen und ihre Erfahrungen zurückgreifen können.

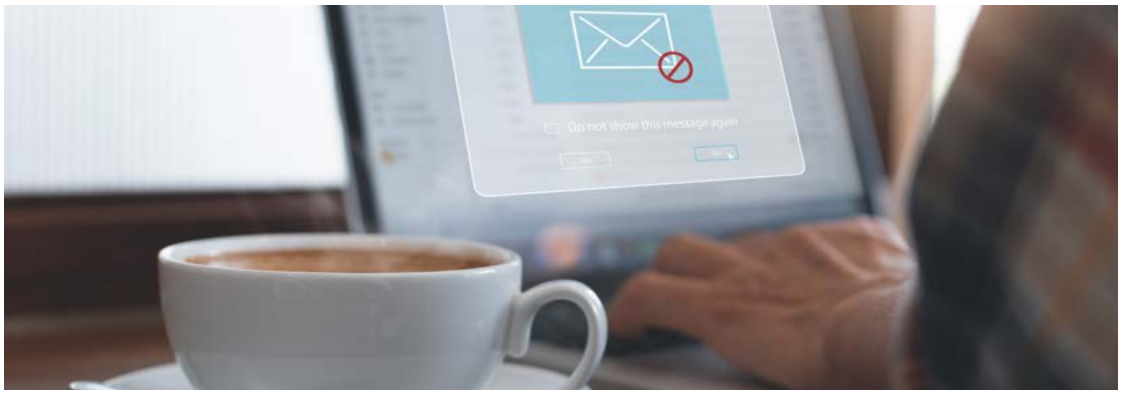
Open-Source-E-Mail-Systeme und Souveränität

Die Sicherheit von geschäftlichen E-Mails muss auf verschiedenen Ebenen gewährleistet werden. Es ist wichtig, sich zu fragen, wo die Daten gespeichert werden. Wie kann auf sie zugegriffen werden? Bei Open-Source-Lösungen werden den Unternehmen keine festen Vorgaben auferlegt. Demnach können Sie frei wählen, welchen Datenhoster Sie nutzen und sicherstellen, dass die Daten ordnungsgemäß verwaltet werden.

Um den Betrieb der E-Mail-Dienste im Falle eines Störfalls zu gewährleisten, können Sie mit Ihrem Hosting-Anbieter einen „Business Recovery Plan“ abschließen. Die Wahl eines europäischen Open-Source-E-Mail-Systems in Verbindung mit einem souveränen Hosting stellt eine wesentliche Grundlage für die Sicherheit dar. Die Daten des Unternehmens fallen dann nicht unter die Bestimmungen des Cloud-Acts, der für die großen Messaging-Anbieter wie die GAFAM gilt.

Auch wenn es in der Cybersicherheit kein Null-Risiko gib: Hacker konzentrieren sich bevorzugt auf große und führende Anbieter. Dieses Risiko kann mit einem umfassenden Arsenal an E-Mail-Sicherheitsmaßnahmen verringert werden.

Des Weiteren muss das E-Mail-System in die IT-Architektur des Unternehmens integriert werden, um mit anderen Tools kommunizieren zu können. **Open Source ist auch in diesem Fall eine interessante Alternative**.



Das Beispiel von SOGo Webmail

SOGo ist eine Open-Source-Webmail-Lösung, die die gemeinsame Nutzung von Kalendern, Adressbüchern und E-Mails innerhalb eines Unternehmens erlaubt. Die Lösung ist für Organisationen kostenfrei, wenn sie diese selbst installieren und einsetzen möchten.

SOGo ist eine universelle und responsive Webmail-Lösung, die auf AJAX basiert. Die Frontend-Komponente der Messaging-Infrastruktur stellt den Nutzern eine vollständige Schnittstelle für den Informationszugang bereit. SOGo verfügt über eine engagierte Community von mehreren Tausend Entwicklern, die kontinuierlich an der Verbesserung der Lösung arbeiten.

Alinto bietet seit 2022 eine professionelle Cloud-Lösung von SOGo mit dediziertem Support und 24/7-Monitoring an. Eine ideale Lösung für Unternehmen, die eine vollständige Integration und Unterstützung beim Betrieb der Lösung suchen. **SOGomail ist absolut sicher, und basiert auf einem souveränen Hosting-Service**.

Auf dem Weg zur digitalen Souveränität kommt dem Messaging eine wichtige Rolle zu. Open-Source-Software in Kombination mit europäischen Cloud-Hosting-Diensten ist eine Möglichkeit, dies zu erreichen. Unternehmen setzen zunehmend auf diese Technologien. Obwohl die Umstellung aufgrund der Trägheit der Lebenszyklen von Lösungen und Markterneuerungen Zeit in Anspruch nehmen kann, ist der Trend deutlich erkennbar.

Fazit

Unternehmen legen zunehmend Wert auf digitale Souveränität. Hierfür gibt es viele Gründe:

Der Wunsch, die Kontrolle über die eigenen Daten zu behalten, die Verwendung europäischer Software zu fördern oder die Unabhängigkeit von großen amerikanischen und anderen globalen Anbietern zu gewährleisten.

Die europäischen Regierungen unterstützten zunehmend Open-Source-Initiativen. Gleichzeitig zögern immer weniger Unternehmen, sie zu nutzen. Es ist in ihrem eigenen Interesse, diese Optionen zu nutzen, um die Kontrolle über ihre Daten zu behalten. Und das beginnt bei Business Messaging und seiner Sicherheit.

Über uns

Alinto wurde im Jahr 2000 gegründet und ist ein Unternehmen, das sich auf E-Mail-Lösungen spezialisiert hat und sowohl SaaS als auch PaaS-Modelle für E-Mail- und Sicherheitsdienste anbietet. Diese werden durch mehrere Produkte abgedeckt.

- **SOGomail** ist ein sicherer und kollaborativer All-in-One-Mailserver, der das vollständig responsive SOGo Mail integriert.

- **Cleanmail** ist eine E-Mail-Relay-Plattform, die einen sicheren Schutz vor Cyber-Bedrohungen gewährleistet und einen kontinuierlichen Zugriff auf E-Mails garantiert.

- **Serenamail** ist ein SMTP-Relay, das es Servern oder Anwendungen ermöglicht, E-Mails zu versenden und einen „sauberen“ E-Mail-Traffic garantiert.

Alinto, der europäische Spezialist für sichere E-Mail-Lösungen, reagiert auf die neuen Marktanforderungen, indem er sich verstärkt Open Source zuwendet. Der Software-Hersteller hat das SOGo-Webmail und dessen Community sowie die E-Mail-Filterung übernommen.

Warum ist die Entscheidung für Open-Source so wichtig? Es ist vorwiegend eine Frage der digitalen Souveränität. Open-Source-Software ist Software, deren Quelltext den Nutzern zugänglich ist und die von Unternehmen betrieben werden kann, die die Kontrolle über das Hosting, die Speicherung, den Betrieb und die Reversibilität der Daten behalten möchten. Für Alinto ist Open Source ein Instrument, um seinen Kunden und Partnern digitale Souveränität zu garantieren. Dies ist auch die Möglichkeit, eine starke und nachhaltige Alternative zu GAFAM anzubieten.

„Unserer Meinung nach ist Open-Source ein wichtiges Element, um den Nutzern die größtmögliche Auswahl zu bieten. Es ist ein wichtiges Element für die Diversität und eine Möglichkeit für uns, Unternehmen Alternativen zu den Messaging-Tools der amerikanischen Cloud-Anbieter anzubieten“, sagt **Philippe Gilbert, CEO von Alinto**.

Lyon (Firmenzentrale)
15 quai Tilsitt
FR-69002 Lyon
+33 481 09 01 10

Barcelona
Paseo de Gracia,101-4°1
SP-08008 Barcelona
+34 91 005 29 64

Zürich
Gertrudstrasse 1
CH-8400 Winterthur
+41 52 208 99 66

Lausanne
Rue des Jordils 40
CH-1025 St-Sulpice
Tel: +41 21 695 20 20

Alinto

www.alinto.com