Überblick über die Informationssicherheit bei Elastic Cloud

Oktober 2023

elastic.co/de

INHALTSVERZEICHNIS

Leistungen und Umfang

Mit Lösungen für Enterprise Search, Observability und Security unterstützen wir Nutzer:innen dabei, schneller zu finden, wonach sie suchen, missionskritische Anwendungen am Laufen zu halten und sich vor Cyberbedrohungen zu schützen. Elastic Cloud ist so gestaltet, dass Sie die Freiheit haben, Deployments auf Ihren ganz konkreten Anwendungsfall zuzuschneiden und Ihren Anforderungen entsprechend zu verwalten. Dabei wird dafür gesorgt, dass die Abläufe einfach gehalten werden und die Geschwindigkeit, Skalierbarkeit und Relevanz der den Sucherlebnissen zugrunde liegenden Plattform aufrecht erhalten bleibt.

Wir sind uns der großen Verantwortung bewusst, die wir gegenüber Ihnen, unseren Kunden, haben. Schließlich verlassen Sie sich darauf, dass wir Ihnen hervorragende Sucherlebnisse bereitstellen und gleichzeitig Ihre Daten schützen. Wir arbeiten mit ganzer Kraft daran, dieses Vertrauen nicht zu enttäuschen. Sicherheitsbelange – von der Beaufsichtigung durch den Aufsichtsrat und der Führung durch die Geschäftsleitung an der Spitze des Unternehmens bis hinunter zur Art und Weise, wie wir bei Elastic jede Mitarbeiterin und jeden Mitarbeiter einarbeiten und kontinuierlich schulen – sind für uns in jeder einzelnen Phase unserer Arbeit von herausragender Bedeutung. Dass es uns gelingt, ein höchstmögliches Maß an Sicherheit aufrechtzuerhalten, zeigen zahlreiche Compliance-Berichte und Zertifizierungen für Elastic Cloud sowie unser Information Security Management System (ISMS) durch führende Anbieter. Diese Berichte und Zertifizierungen zeugen davon, dass alle unsere Aktivitäten – von der Produktentwicklung und -bereitstellung über das Schwachstellenmanagement und das Incident-Management bis hin zu den Prozessen zum Umgang mit Bedrohungen – von wirksamen Sicherheitsmaßnahmen begleitet werden.

In diesem Dokument umreißen wir die Richtlinien, Prozeduren und technischen Maßnahmen, die bei Elastic in Kraft sind, damit Sie Elastic Cloud mit vollem Vertrauen für Ihre Lösungen nutzen können. Um die vielfältigen Anforderungen von Nutzer:innen und Kunden befriedigen zu können, lassen sich Elastic Cloud und die zugehörigen Softwarelösungen lokal („on-premises“), in öffentlichen oder privaten Clouds oder in hybriden Umgebungen bereitstellen. Bitte beachten Sie, dass in diesem Dokument keine Sicherheitsmaßnahmen besprochen werden, die ausschließlich auf selbstverwaltete Deployments zutreffen.

Überblick über Elastic Cloud

Elastic liefert cloudnative Lösungen für Enterprise Search, Observability und Security für schnelle und einfache Suchen, für den unterbrechungsfreien Betrieb missionskritischer Anwendungen und für den Schutz vor Cyberbedrohungen. Elastic-Produkte ingestieren und speichern Daten aus allen Quellen und in allen Formaten, um Suchen, Analysen und Visualisierungen zu ermöglichen.

Elastic Cloud ist eine Familie von Software-as-a-Service(SaaS)-Produkten: Elasticsearch Service (ESS), Enterprise Search, Observability und Elastic Security. Elastic hostet und verwaltet Elastic Stack-Komponenten, einschließlich Elasticsearch und Kibana, auf vom Kunden ausgewählter Infrastruktur bei mehreren Anbietern öffentlicher Clouds, namentlich Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure und IBM. Im Rahmen der Elastic Cloud-Angebote können über das Elastic Stack-Basisangebot hinausgehende Features wie Security-, Alerting-, Monitoring-, Reporting-, Machine-Learning- und Visualisierungsfunktionen genutzt werden.

Die folgende Tabelle gibt einen Überblick über die Komponenten von Elastic Cloud.

Elastic Cloud-Komponente	**Beschreibung**
Elasticsearch Service (ESS)	ESS ist ein verteilter Dienst, der als Echtzeit-Suchmaschine, Analytics-Engine und Datenspeicher für Daten aller Art fungiert – von Textdaten über numerische Daten und Geodaten bis hin zu strukturierten und unstrukturierten Daten.
Enterprise Search	Elastic Enterprise Search bietet leistungsstarke Tools für die schnelle Bereitstellung von Sucherlebnissen mit nahtloser Skalierbarkeit: *Workplace Search* ist ein Tool, das die Content-Plattformen von Unternehmen (Google Drive, Slack, Salesforce und viele andere) in einem personalisierten, natürlichen Sucherlebnis zusammenführt. *App Search* ist ein Paket von Tools für Entwickler:innen, das die Leistungsfähigkeit von Elasticsearch nutzt, um mobile und SaaS-Anwendungen mit Suchfunktionen zu versorgen – inklusive Web-Crawler, leistungsstarken APIs, intuitiven Dashboards und justierbaren Relevanzeinstellungen. Mit *Site Search* können Sie Ihren Websites leistungsfähige Suchfunktionen hinzufügen – auch ein Suchfeld, wenn nötig.

Observability	Elastic Observability bietet zentralisierte Analysefunktionen für Logdaten, Metriken, APM-Traces und Uptime-Informationen. Unternehmen, die Elastic Agent und die vordefinierten Integrations-Connectors für die Datenerfassung nutzen, können mithilfe von Machine Learning und vordefinierten Erkennungsregeln Verhaltensanomalien erkennen, wovon sowohl DevOps- als auch SecOps-Teams profitieren.
Security	Elastic Security bietet Funktionen zur Vermeidung, Erkennung und Behebung von Bedrohungen, die alle über dieselbe Benutzeroberfläche genutzt werden können: *Elastic SIEM* verfügt über Funktionen für die konventionelle Aggregation und Korrelation von Logdaten und unterstützt damit die Erkennung und Bekämpfung von Bedrohungen sowie über erweiterte Security-Features, wie die Machine-Learning-gestützte Risikobewertung, integriertes Case Management und SOAR. *Elastic Agent* bietet trotz minimalem Ressourcenbedarf grenzenlose Vielseitigkeit und kann praktisch überall eingesetzt werden, auch in hybriden Umgebungen. Der Agent kann Bedrohungen vorbeugen, Daten weiterleiten und mehrere Anwendungsfälle unterstützen, um Security-Informationen anzureichern und Schutzmaßnahmen wirksamer zu machen. *Limitless XDR* modernisiert Security-Abläufe, indem es SIEM und Endpoint-Security zentralisiert, Analysen anhand von Datenbeständen aus vielen Jahren ermöglicht, Erkennungs- und Bekämpfungsprozesse automatisiert und nativen Endpoint-Schutz auf jeden Host bringt.

Cloud-Compliance-Programme

Elastic Cloud ist so konzipiert, dass die Sicherheit an erster Stelle steht. Unsere Produkte und Dienste wurden und werden von führenden Anbietern zertifiziert und attestiert und deren Berichte belegen unser Engagement für Sicherheit, Compliance, Datenschutz und Zuverlässigkeit.

Das globale ISMS von Elastic hat eine ISO-27001-Zertifizierung erhalten, und für den kommerziellen Elastic Cloud-Dienst liegen Zertifizierungen bzw. Attestierungen nach ISO 27017, ISO 27018, SOC 2 Type 2, CSA Cloud Compliance Matrix (CCM), HIPAA und PCI-DSS vor. Darüber hinaus können wir Executive Summarys für Penetrationstests sowie branchen- und länderspezifische Zertifizierungen (z. B. TISAX) vorlegen. Mehr über die Compliance-Standards, auf die wir geprüft werden, und darüber, wie Sie an die erwähnten Berichte und Zertifizierungen gelangen, erfahren Sie im Abschnitt „Compliance-Standards“ dieses Dokuments.

Darüber hinaus ist Elastic Cloud in AWS GovCloud mit der Einstufung „Moderate Impact“ FedRAMP-autorisiert. Näheres zu dieser Zertifizierung erfahren Sie auf der Webseite zu unserem FedRAMP-autorisierten Cloud-Angebot. Bestehende und potenzielle Kunden, die das FedRAMP-autorisierte Angebot nutzen möchten, können über das Formular „FedRAMP Package Access Request Form“ im FedRAMP Marketplace Zugriff auf unsere FedRAMP Security Packages beantragen.

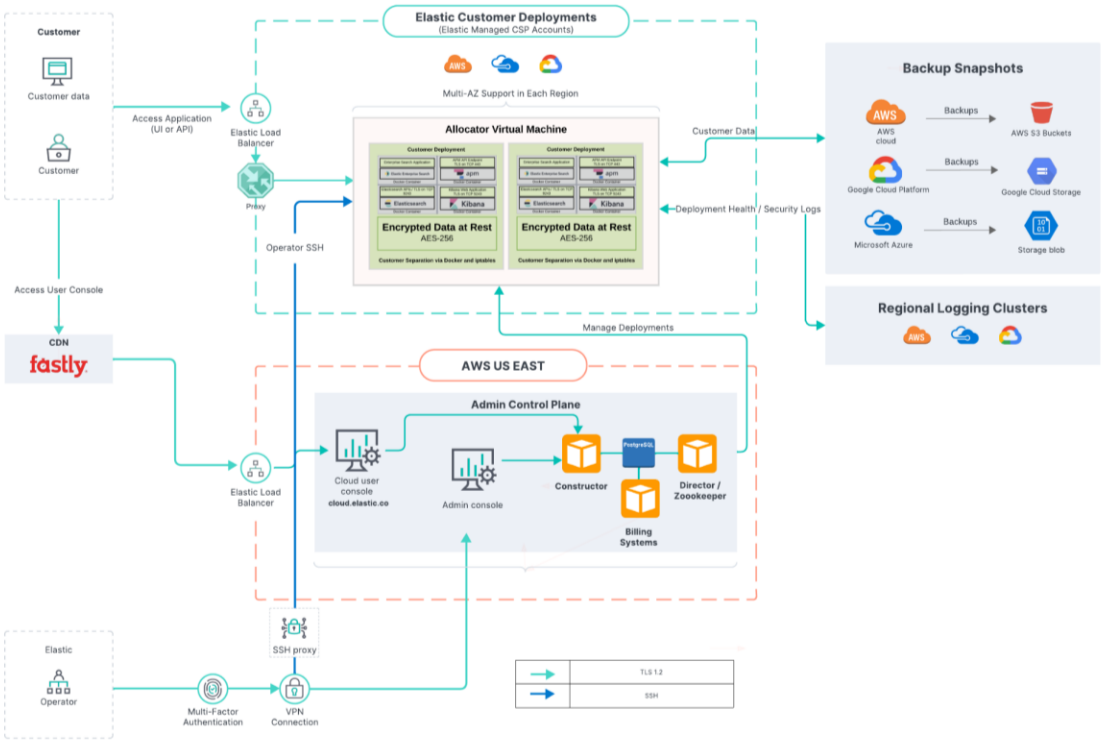
Produktnutzungsdaten und Kundeninhalte

Wir behandeln die Informationen unserer Kunden mit größter Sorgfalt – die in diesem Dokument beschriebenen Schutzmaßnahmen dienen dazu, Kundeninhalte zu schützen. Im Folgenden beschreiben wir die Unterschiede zwischen Produktnutzungsdaten und Kundeninhalten.

Produktnutzungsdaten: Dies sind die Daten, die Elastic verwendet, um Produkte bereitstellen, die Infrastruktur verwalten und überwachen, Support leisten und Produkte analysieren und verbessern zu können. Produktnutzungsdaten unterliegen strengen Zugriffsregeln und Schutzmaßnahmen und ihre Sicherheit und Integrität wird sowohl intern als auch extern geprüft. In diesem Dokument soll es jedoch in erster Linie darum gehen, wie wir „Defense-in-Depth“-Maßnahmen nutzen, um Kundeninhalte zu schützen.

Kundeninhalte: Dies sind die Daten, die Kunden ingestieren, hochladen oder anderweitig in Elastic-Produkte und -Dienste importieren. Elastic verarbeitet diese Daten nur so weit, wie es für die Bereitstellung der Produkte oder Dienste sowie gegebenenfalls für die Einhaltung der gesetzlichen Vorschriften erforderlich ist. Der Kunde hat jederzeit die volle Kontrolle darüber, welche Daten in Elastic Cloud ingestiert werden sollen.

Diagramm des Elastic Cloud-Dienstes



Beschreibung der Elastic Cloud-Architektur

Steuerungsebene

Auf der Steuerungsebene von Elastic Cloud befinden sich die Verwaltungsdienste **ZooKeeper**, **Director** und **Constructor**, die im Folgenden näher beschrieben werden:

- **ZooKeeper:** ZooKeeper ist ein verteilter Datenspeicher, in dem wichtige Informationen für Elastic Cloud-Komponenten gespeichert sind: Proxy-Routing-Tabellen, von den Verteilern (Allocators) als frei gemeldete Arbeitsspeicherkapazität, via Admin-Konsole abgesendete Änderungen und so weiter. Er fungiert als Nachrichtenbus für die Kommunikation zwischen den Diensten. Außerdem speichert er Informationen zum Zustand der Elastic Cloud-Installation und zum Zustand aller in Elastic Cloud laufenden Deployments.

- **Director:** Director verwaltet den ZooKeeper-Datenspeicher und signiert die Certificate Signing Requests (CSRs) für interne Clients, die mit ZooKeeper kommunizieren möchten. Die Komponente kümmert sich auch um die STunnels, die ZooKeeper für die Kommunikation nutzt, und um die Quorum-Verwaltung bei der Erstellung neuer ZooKeeper-Knoten.

- **Constructor:** Constructor übernimmt die Rolle eines Zeitplaners (Scheduler), der von der Admin-Konsole kommende Anfragen überwacht. Die Komponente ermittelt, was geändert werden muss, und schreibt diese Änderungen in die ZooKeeper-Knoten, die von den Allocators überwacht werden. Außerdem weist sie Allocators Cluster-Knoten zu und sorgt für eine maximale Auslastung der zugrunde liegenden Allocators, um zu verhindern, dass bei neuen Deployments zusätzliche Hardware hinzugezogen werden muss. Der Constructor platziert Cluster-Knoten und Instanzen in unterschiedlichen Verfügbarkeitszonen, damit ein eventueller Ausfall einer Zone dem Deployment nichts anhaben kann.

  Zur Aufrechterhaltung der Datensouveränität können diese Platzierungspräferenzen kundenseitig angepasst werden.

- **Cloud-Benutzeroberfläche und -API:** Diese Features ermöglichen Administratoren den Web- und API-Zugriff zum Verwalten und Überwachen ihrer Installation.

Proxys

Die Aufgabe von Proxys besteht darin, die in Anfrage-URLs von Nutzeranfragen für den Container übergebenen Deployment-IDs den eigentlichen Elasticsearch-Cluster-Knoten und anderen Instanzen zuzuordnen. Die Zuordnung von Deployment-IDs zu einem Container wird in ZooKeeper gespeichert und von den Proxys im Cache zwischengespeichert. Dank des Caches kann die Plattform bei einem Ausfall von ZooKeeper die Anfragen für bestehende Deployments weiterhin bedienen.

Bei hochverfügbaren Elasticsearch-Clustern überwachen Proxys auch jederzeit den Zustand und die Verfügbarkeit der Zonen. Wenn eine der Zonen ausfällt, werden keine Anfragen an diese Zone geleitet. Darüber hinaus ermöglichen Proxys auch Skalierungen und Upgrades, ohne dass Systeme oder Dienste offline gehen müssen. Vor der Durchführung eines Upgrades wird ein Snapshot erstellt und Daten werden auf die neuen Knoten migriert. Nach Abschluss der Migration schaltet ein Proxy den Traffic auf die neuen Knoten um und trennt die Verbindung zu den alten Knoten. In der Regel werden zur Aufrechterhaltung der Systemverfügbarkeit hinter einem Load Balancer mehrere Proxys konfiguriert.

Allocators

Allocators (Verteiler) werden auf allen Maschinen ausgeführt, auf denen Elasticsearch-Knoten und Kibana-Instanzen gehostet werden. Sie steuern den Lebenszyklus von Cluster-Knoten und führen dazu die folgenden Aktionen aus:

- Erstellen neuer Container und Starten von Elasticsearch-Knoten auf entsprechende Anfrage
- Neustarten von Knoten, wenn diese nicht mehr ordnungsgemäß reagieren
- Entfernen von Knoten, die nicht mehr benötigt werden

Sie informieren ZooKeeper auch über die Arbeitsspeicherkapazität der zugrunde liegenden Host-Maschine, damit der Constructor entscheiden kann, wo die Bereitstellung erfolgen soll.

Risikomanagement

Elastic nutzt für die Aufrechterhaltung von Security und Compliance eine risikobasierte Herangehensweise unter Verwendung von FAIR, dem führenden Verfahren zur quantitativen Bewertung und Analyse von Geschäftsrisiken und zur Priorisierung von Risikominderungsmaßnahmen.

Der Risikobewertungsprozess von Elastic identifiziert und verwaltet Risiken, die sich auf Ihre Fähigkeit auswirken könnten, Ihren Kund:innen vertrauenswürdige und zuverlässige Leistungen bereitzustellen. Im Folgenden haben wir die wichtigsten Risiken zusammengefasst, die wir ermittelt haben und auf deren Eindämmung wir uns in erster Linie konzentrieren:

- Leitung und Verwaltung der Organisation
- Sicherheit des Personals
- Asset Management
- Zugriffssteuerung
- Kryptografie
- Sicherheit der Kommunikation
- Beschaffung, Entwicklung und Pflege von Systemen
- Lieferantenbeziehungen
- Management von Vorfällen (Incidents) im Zusammenhang mit der Sicherheit von Informationen
- Business-Continuity-Management

Bei der Risikoidentifizierung werden sowohl interne als auch externe Faktoren sowie deren Auswirkungen auf die Erreichung der Ziele berücksichtigt.

Identifizierte Risiken werden durch einen Prozess analysiert, bei dem die möglichen Bedrohungen und Schwachstellen in Bezug auf Ihre Geschäftsziele analysiert werden und die potenzielle Signifikanz des Risikos eingeschätzt wird. Im Rahmen der Risikobewertung wird betrachtet, wie das Risiko verwaltet werden kann und ob es akzeptiert, vermieden, gemindert oder übertragen werden sollte. Für die identifizierten Risiken werden Risikominderungsstrategien ermittelt. Diese können das Entwerfen, Entwickeln und Umsetzen von Risikosteuerungsmaßnahmen sowie das Einführen bzw. Überarbeiten von Richtlinien und Verfahren beinhalten.

Der kollektive Prozess zur Identifizierung, Analyse und Bewertung von Risiken stellt Informationen für unser Risikoregister (Risk Register) bereit. Dieses enthält Risikoszenarien, die mit dem FAIR-Verfahren evaluiert und auf der Basis der geschätzten finanziellen Auswirkungen für Elastic in ein Prioritäts-Ranking eingeordnet werden. Das Risk Register wird halbjährlich einer Evaluierung unterzogen, um Änderungen bei internen oder externen Risikofaktoren und Geschäftsprioritäten sowie dynamischen Risikominderungsstrategien Rechnung zu tragen. Dieser Prozess bildet auch die Grundlage für die risikobasierte Herangehensweise bei der Berichterstattung durch das Informationssicherheitsteam gegenüber dem Audit Committee des Board of Directors.

Governance

Information Security Management System (ISMS) und Aufsicht

Elastic verfügt über ein ISMS, das Richtlinien, Verfahren, operative Strukturen und technische Maßnahmen umfasst, die in ihrer Gesamtheit zum Schutz von Kunden- und Unternehmensdaten beitragen. Das ISMS ist nach ISO 27001 zertifiziert und so organisiert, dass es alle Security- und Compliance-Bereiche abdeckt, von Governance und Vertrauen über das Risiko- und Schwachstellenmanagement bis hin zu Dingen wie Sicherheitsarchitektur und -Engineering, Produktsicherheit, Bedrohungserkennung und Reaktion auf Sicherheitsvorfälle.

Das ISMS unterliegt der Aufsicht des Board of Directors (Audit Committee) von Elastic. Das Audit Committee trifft sich regelmäßig mit dem Chief Information Security Officer (CISO), um die Ausrichtung des Informationssicherheitsprogramms an den kurz- und langfristigen Geschäftszielen sicherzustellen und sich zu vergewissern, dass Best Practices der Branche befolgt werden und sich die Maßnahmen mit der dynamischen Bedrohungslandschaft mitentwickeln.

Zur Unterstützung des Elastic-eigenen ISMS wurde ein Business Integrity and Privacy Team eingerichtet, das in enger Zusammenarbeit mit dem Information Security Team an organisatorischen Lösungen arbeitet, die die Einhaltung der in der Welt geltenden Datengesetze und -vorschriften sicherstellen.

Richtlinien für die Informationssicherheit

Elastic hat einen umfassenden Bestand an Richtlinien entwickelt, die die Grundlage für die Informationssicherheitspraktiken von Elastic bilden, auf Industrienormen wie NIST und ISO 27001 basieren und gegenüber den Mitarbeitenden im Unternehmen kommunizieren, was seitens der Geschäftsführung erwartet wird. Diese Richtlinien werden von den für sie Verantwortlichen einmal jährlich überprüft und von der Geschäftsführung bestätigt. Die Richtlinien von Elastic betreffen die folgenden Bereiche:

- Informationssicherheitsprogramm
- akzeptable Nutzung
- Risikomanagement
- Asset Management
- Datenklassifizierung
- Datensatzaufbewahrung
- Zugriffssteuerung
- Workstation- und Server-Sicherheit
- Security Analysis und Logging
- Schwachstellenmanagement
- Change Management
- Secure Software Development
- Incident Response
- Business Continuity und Disaster Recovery

Alle Mitarbeitenden von Elastic müssen bei der Einstellung und nachfolgend einmal pro Jahr bestätigen, dass sie den Elastic-Verhaltenskodex sowie die Richtlinien zur Informationssicherheit, zum Datenschutz und zur akzeptablen Nutzung gelesen haben und sich an diese Vorgaben halten werden.

Der vollständige Text unserer Richtlinien für die Informationssicherheit ist nicht für die Öffentlichkeit bestimmt. Es kann aber ein so genanntes „Information Security Policies Bundle“ zur Verfügung gestellt werden, das die Inhaltsverzeichnisse der Richtlinien sowie Angaben zu den Versionshistorien enthält und damit Aufschluss über die in den Richtlinien behandelten Themengebiete gibt und die Einhaltung der Vorgaben zur regelmäßigen Überprüfung, Überarbeitung und Genehmigung belegt. Dieses Dokument erhalten Sie über Ihren Elastic Account Representative oder über den Elastic Support.

Zusätzlich zu den formellen Richtlinien gibt es bei Elastic auch regelmäßig aktualisierte Playbooks, Prozessdokumente und Pläne für Bereiche mit ganz eigenen Prozessanforderungen bzw. sich dynamisch entwickelnden Best Practices, wie Cloud-Verschlüsselung, Zertifikats- und Schlüsselverwaltung und Management des Risikos durch Dritte (Third Party Risk Management).

Human Resource Management

Uns ist bewusst, dass es für den Erfolg eines umfassenden Security-Programms einer entsprechenden Ansage aus der Geschäftsführung bedarf und dass ein solches Programm nur gelingen kann, wenn alle Mitarbeitenden mitmachen. Unser Quellcode, unser „Employee Handbook“ und unser Verhaltenskodex enthalten klare Vorgaben und ethische Normen, die von allen Mitarbeitenden bei Elastic einzuhalten sind. Verstöße gegen diese Vorgaben und Normen werden ohne Ausnahme und unabhängig von Position, Dienstalter oder Amtszeit geahndet.

Elastic hat darüber hinaus Sicherheits-Best-Practices für die einzelnen Organisationseinheiten des Unternehmens mit formellen Berichtslinien aufgestellt, die für den Fluss von Informationen an die relevanten Personen sorgen sowie die entsprechende Verantwortlichkeit und Beaufsichtigung des Verhaltens und der Leistung der Mitarbeitenden sicherstellen sollen. Rollen und Verantwortlichkeiten sind auf Basis der Anforderungen der Funktion getrennt und die Jobrollen sind ausdrücklich definiert.

Die Einstellung und Kündigung von Mitarbeitenden erfolgt in Übereinstimmung mit dokumentierten Richtlinien und Verfahren, einschließlich von Verfahren für das sichere und schnelle On- und Offboarding festangestellter und freier Mitarbeitender.

Zu den Security-Best-Practices auf unterer Organisationsebene gehören zudem Prüfungen des Hintergrunds neuer festangestellter und freier Mitarbeitender vor Aufnahme der Tätigkeit. Hinzu kommen für alle Elastic-Mitarbeitenden, einschließlich der obersten Ebenen der Geschäftsführung, bei der Einstellung und anschließend im jährlichen Rhythmus obligatorische Schulungen zur Schärfung des Bewusstseins für Sicherheitsbelange (Security Awareness) sowie die Pflicht, die Richtlinien zur Informationssicherheit und zum Datenschutz, den Verhaltenskodex und das „Employee Handbook“ zu lesen und sich zu deren Einhaltung zu bekennen.

Asset Management

Der Asset-Management-Lebenszyklus unterliegt dem Asset Management Standard; dieser umfasst ein Inventar der Vermögenswerte (Assets), Angaben zur Eigentümerschaft der Assets sowie zur Rückgabe und Entsorgung von Assets sowie die Protokollierungsanforderungen. Die Asset-Management-Prozesse beim Flottenmanagement unterscheiden sich von denen beim Endpoint-Management. Im Folgenden werden die beiden Prozesse näher erläutert:

Flottenmanagement

Die Anbieter von Cloud-Diensten (Cloud Service Providers, CSPs), mit denen wir zusammenarbeiten – AWS, GCP, Azure und IBM – verwalten die Infrastruktur, die der Elastic Cloud zugrunde liegt. Elastic Cloud-Kunden können für jedes ihrer Deployments flexibel wählen, welchen CSP und welche geografische Region sie für ihre Daten nutzen möchten. Physische Sicherheitsmaßnahmen sowie Maßnahmen zur Steuerung des Medien- und Hardwarezugriffs obliegen dem jeweiligen CSP. Elastic überprüft bei Drittanbieter-Rezertifizierungen im Rahmen unseres „Third Party Risk Management“-Programms regelmäßig das Design und die operative Wirksamkeit der von den CSP-Partnern ergriffenen Maßnahmen zur Steuerung des Medien- und Hardware-Lifecycle-Managements.

Zur Verfolgung der Performance- und Uptime-Metriken der Elastic-Cluster kommt Elastic Observability zum Einsatz. Kritische Assets werden im Asset Inventory registriert. Dieses wird regelmäßig auf Vollständigkeit und Korrektheit geprüft.

Endpoints bei den Mitarbeitenden

Elastic IT verfolgt und verwaltet die an die Mitarbeitenden ausgegebenen Endpoints von einer zentralen Stelle aus. Mittels Software zur Geräteverwaltung wird dafür gesorgt, dass die vorgegebenen Sicherheitseinstellungen durchgesetzt werden. Verschlüsselung, Passwortverwaltung, Sitzungsverwaltung und Bildschirmsperrung sind standardmäßig aktiviert. Diese Einstellungen können weder deaktiviert noch lokal geändert werden. Endpoints werden durch Elastic Security geschützt, das EDR-Funktionen sowie Echtzeit-Monitoring und Alerting bietet. Mehr darüber, wie wir die Endpoints von Mitarbeitenden vor Malware schützen, erfahren Sie im Abschnitt „Schutz vor Malware“.

Für alle von Elastic ausgegebenen Geräte gilt unser Gerätemanagement-Lebenszyklus. Wenn ein:e Mitarbeitende:r von Elastic das Unternehmen verlässt, wird ihr bzw. sein logischer Zugriff deaktiviert und die vom Unternehmen verwalteten Endpoints werden direkt an einen externen Dienstleister gesendet, der die erforderlichen Schritte zur Löschung und Zerstörung der Daten unternimmt.
Der externe Dienstleister legt Elastic entsprechende Zerstörungszertifikate vor und setzt das Gerät gemäß dem Elastic Laptop Handling Standard wieder auf seinen Ausgangszustand zurück oder entsorgt es. Elastic IT unterhält ein Protokoll der von Elastic verwalteten Endpoints, um den Status jedes einzelnen Geräts innerhalb des Datenzerstörungs-Lebenszyklus verfolgen zu können.

Die Richtlinien schreiben vor, dass auf nicht verwalteten oder persönlichen Mobilgeräten keine Kundendaten gespeichert werden und solche Geräte auch nicht bei der Entwicklung oder beim Support von Elastic Cloud zum Einsatz kommen dürfen.

Konfigurationsmanagement

Das Konfigurationsmanagement bei Elastic erfolgt per Code und Konfigurationsänderungen richten sich nach dem für das Change Management geltenden Standardverfahren mit Autorisierung, Peer Review und Genehmigung sowie automatisierten Test-Suites. Elastic setzt File Integrity Monitoring ein, um nach direkten Änderungen bei Produktionskonfigurationsdateien sowie nach verdächtigen Aktivitäten zu suchen.

Datenschutz

Klassifizierung und Aufbewahrung von Daten

Der Elastic Data Classification Standard sieht vor, dass Daten gemäß ihrer Sicherheitsrelevanz klassifiziert werden müssen und dass für jede Klassifizierungsstufe Zugriffs- und Weitergabeeinschränkungen zu definieren sind. Kundeninhalte und Produktnutzungsdaten werden mit der höchsten Sicherheitsrelevanzstufe „restricted“ (eingeschränkter Zugriff) klassifiziert und unterliegen damit den strengsten Datenschutznormen, um die Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten zu bewahren. Definitionen der Begriffe „Kundeninhalte“ und „Produktnutzungsdaten“ finden Sie im Abschnitt „Produktnutzungsdaten und Kundeninhalte“ dieses Dokuments.

Im Elastic Record Retention Standard ist festgeschrieben, dass Daten nach Ablauf der für den jeweiligen Datentyp und die betrieblichen, vertraglichen, rechtlichen und regulatorischen Anforderungen geltenden definierten Aufbewahrungszeiträume gelöscht werden müssen. Kunden, die ihre Daten gelöscht sehen möchten, können beim Elastic Support jederzeit eine Löschung ihres Kontos anfordern. Wie Sie den Zugriff auf Ihre Daten anfordern können, erfahren Sie im Abschnitt „Sicherheit und Schutz der Daten“ dieses Dokuments.

Erfassung, Verarbeitung und Entsorgung von Daten

Datenerfassung

Elastic erfasst nur die Informationen, die für die Bereitstellung, Unterstützung, Aufrechterhaltung, Absicherung und Verbesserung seiner Dienstleistungen erforderlich sind. Diese Informationen werden niemals an Dritte verkauft. Mehr darüber, welche Informationen wir von Kunden erfassen, erfahren Sie in unserem „Product Privacy Statement“.

Dateningestion

Elastic hat weder Einfluss auf die Daten, die Kunden auf Ihrem Elastic-Deployment speichern oder verarbeiten bzw. dorthin übertragen, noch greift es auf diese zu. Welche Daten vom Elastic-Deployment eines Kunden ingestiert werden, obliegt zu jedem Zeitpunkt einzig der Entscheidung und Kontrolle des Kunden.

Datenzerstörung

Welche Anforderungen für die Zerstörung von Daten gelten, wird durch den Elastic Record Retention Standard und den Elastic Asset Management Standard geregelt. Die sichere Löschung und Zerstörung von Daten, die Teil der Hosting-Infrastruktur sind, liegt in der Verantwortung unserer CSP-Partner. Kunden haben die volle Kontrolle über die Inhalte, die sie in ihren Elastic-Instanzen speichern, und sie haben jederzeit das Recht, Inhalte aus ihren Elastic-Instanzen zu entfernen oder zu löschen.

Verschlüsselung

Verschlüsselung während der Übertragung (Encryption in-transit)

Das Verschlüsselungsprotokoll TLS (Transport Layer Security) sorgt standardmäßig dafür, dass die Daten in Elastic Cloud während der Übertragung verschlüsselt werden. Die Verschlüsselungsstärke muss dabei mindestens TLS 1.2 entsprechen. TLS-(HTTPS)-Verbindungen werden im Elastic Cloud-Service-Diagramm angezeigt.

Die für die Unterstützung von Elastic Cloud verwendeten Zertifikate werden von Digicert ausgestellt und nutzen die RSA-Public-Key-Authentifizierung mit 2048-Bit-Schlüsseln. Elastic verfügt über gültige Zertifikate für seine Cloud-Deployments mit einem Qualys SSL Labs-Rating von A+. Diese Testergebnisse können auf der SSL Labs-Website reproduziert werden.

Verschlüsselung der Daten im Speicher (Encryption at-rest)

Daten, die sich derzeit im Speicher befinden, werden von unseren CSP-Partnern standardmäßig verschlüsselt (Encryption at-rest). Die minimale Schlüssellänge liegt dabei bei allen Partnern bei 256 Bit, wie es die NIST-Richtlinien empfehlen.

Schlüsselverwaltung

Verschlüsselungsschlüssel verlassen niemals den Host, auf dem sie generiert werden. Bei ihnen handelt sich um Einmalschlüssel. Sie werden automatisch generiert, sobald ein Virtual-Machine-Host erstellt oder ersetzt wird. Die Schlüssel werden weder gesichert noch offengelegt und bleiben immer auf dem Host. Bei der Schlüsselverwaltung für die Verschlüsselung in den zugrunde liegenden IaaS-Diensten handelt es sich um einen automatisierten Prozess, der auf den Schlüsselverwaltungsdienst (Key Management Service) des jeweiligen Anbieters zurückgreift.

Die Schlüsselverwaltung für Elastic-Dienste ist als Infrastructure-as-Code implementiert und in der Betriebsdokumentation für die jeweils betreffende Komponente oder den Dienst dokumentiert.

Netzwerk- und Gerätesicherheitsverwaltung

Firewalls

Die Verwaltung der Hardware-Firewalls für Produktionsinfrastruktur liegt in den Händen unserer CSP-Partner. Elastic unterhält darüber hinaus Software-Firewalls, die unbefugten eingehenden Traffic aus dem Internet herausfiltern und eingehende Netzwerkverbindungen ablehnen, die nicht ausdrücklich autorisiert sind („deny-by-default“). Darüber hinaus sind die logischen Zonen innerhalb der Umgebung durch Netzwerksegmentierung und Firewalls voneinander getrennt. Die Firewall-Regeln werden mindestens einmal pro Halbjahr überprüft. Änderungen bei den Firewall-Regeln unterliegen dem üblichen Change-Management-Prozess und den Kontrollmaßnahmen für das Change Management. Der Zugang zu den Firewalls wird zudem durch die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC) abgesichert.

Zur weiteren Beschränkung des bei ihren Deployments eingehenden Datenverkehrs können Elastic Cloud-Kunden Traffic-Filter einrichten oder AWS PrivateLink konfigurieren.
IP-Traffic-Filter | Elasticsearch Service-Dokumentation | Elastic
AWS PrivateLink-Traffic-Filter | Elasticsearch Service-Dokumentation | Elastic

Schutz vor Malware

Alle Endpoints der Mitarbeitenden sind über zentral verwaltete IT-Konfigurationen mit Anti-Malware-Software versehen. Diese Einstellungen können durch lokale Administrator:innen weder deaktiviert noch geändert werden. Elastic Security Solution bietet EDR-Funktionen und ein rund um die Uhr arbeitendes Team, das Sicherheitsprobleme bearbeitet und Alarmzeichen und -meldungen prüft.

Zum Schutz der Elastic Cloud-Produktionsumgebung wird Elastic Security genutzt. Signaturen und Verhaltensmuster werden automatisch und kontinuierlich aktualisiert. Regeln zur Erkennung neu aufkommender Bedrohungen lassen sich schnell implementieren, und ein eigenes Team für Threat Intelligence, Bedrohungserkennung und Bedrohungsbekämpfung kümmert sich um die Erkennung, Analyse, Bekämpfung und Beseitigung möglicher Malware-Infektionen.

Zeitsynchronisierung

Die Zeitsynchronisierung wird durch NTP mit einer gemeinsamen Zeitquelle (NIST-Server) erreicht.

Logischer Zugriff

Rollenbasierte Zugriffssteuerung

Bei der Vergabe von Zugriffsrechten für interne Nutzer:innen verfolgt Elastic das „Least-Privilege“-Prinzip: Die Mitarbeitenden erhalten nur die Zugriffsrechte, die für die Ausübung ihrer Rolle im Unternehmen erforderlich sind. Die Zugriffsrechte werden regelmäßig überprüft und bei einem Jobwechsel oder unter anderen Umständen, in denen der Nutzerzugriff nicht mehr benötigt wird, entsprechend geändert.

Die Produkte von Elastic verfügen ebenfalls über Funktionen zur rollenbasierten Zugriffssteuerung, damit die Kunden den Nutzer:innen ihrer Elastic-Deployments und der Elastic Cloud-Management-Plattform detaillierte Zugriffsrechte erteilen können.

Neueinstellungen und Entlassungen/Kündigungen

Neuen Mitarbeitenden werden anhand der vorkonfigurierten Regeln in unserem zentralisierten IAM-System (Identity and Access Management) automatisch die entsprechenden Rechte zum Zugriff auf cloudnative SaaS-Anwendungen von Elastic erteilt. Dabei werden Jobattribute aus unserem HR-Aufzeichnungssystem, wie Angaben zur Aufsichtsorganisation, zur Jobfamilie, zur Jobebene und zur Managementstruktur, verwendet, damit jeder und jedem Mitarbeitenden die Zugriffsrechte erteilt werden können, die sie oder er benötigt. Zugriffsrechte, die darüber hinausgehen, müssen formell beantragt und vom Management geprüft und genehmigt werden. Die Beantragung solcher Zugriffsrechte wird in einem Ticket dokumentiert.

Wenn Mitarbeitende zu einer anderen Rolle oder in eine andere Teilorganisation von Elastic wechseln, löst die Änderung ihrer Jobattribute innerhalb des HR-Aufzeichnungssystems im zentralisierten IAM-System automatisch den Workflow zur Neuvergabe von Zugriffsrechten für die betreffenden Mitarbeitenden aus. Die bisherigen Zugriffsrechte werden ihnen entzogen und sie erhalten die Zugriffsrechte, die für die Jobattribute ihrer neuen Rolle definiert wurden.

Nach einer Kündigung des Arbeitsverhältnisses werden die durch unser zentralisierte IAM-System gewährten Zugriffsrechte automatisch aufgehoben, sobald sich der Beschäftigungsstatus in unserem HR-Management-System ändert. Die entsprechende Validierungsprüfung findet mehrmals täglich statt.

Zugriff auf die Produktionsumgebung

Eine begrenzte Zahl von Elastic-Mitarbeitenden darf mit privilegierten Zugriffsrechten auf die Elastic Cloud-Produktionsumgebung zugreifen. Elastic pflegt diese Zugriffsrechte, um die Verwaltung, Wartung und Unterstützung der Plattform zu ermöglichen. Die Elastic Data Handling Policy untersagt Elastic-Mitarbeitenden ausdrücklich, auf Kundendaten zuzugreifen. Das gilt selbst für Wartungs- und Problembehebungsszenarien. Bevor ein:e Elastic-Mitarbeitende:r Einsicht in Daten nehmen kann, die der Kunde freiwillig freigegeben hat, um Unterstützung zu erhalten oder Fehler beseitigt zu bekommen, muss eine schriftliche Einwilligung des jeweiligen Kunden vorliegen. Elastic wird niemals von sich aus auf Kundendaten zugreifen, die in Elastic Cloud ingestiert oder auf Elastic Cloud hochgeladen wurden. Kunden können vor der Freigabe ihrer Daten für Elastic Daten unkenntlich machen oder die freizugebenden Daten bereinigen.

Außerdem hat das Threat Detection and Response Team Erkennungsmechanismen für verdächtige interne Kontoaktivitäten und unbefugte Zugriffe entwickelt. Diese überwachen u. a. die Integrität der Dateien und erkennen Anzeichen für feindliche Kontoübernahmen oder Datenexfiltration. Die genannten Erkennungsmechanismen gehören zu automatisierten Workflows, die das Threat Detection and Response Team über verdächtige Aktivitäten informieren und Untersuchungen durch Analyst:innen auslösen.

Überprüfungen der Zugriffsrechte von Nutzer:innen

Bei der Vergabe von Zugriffsrechten hält sich Elastic an das „Least-Privilege“-Prinzip und gewährt nur die Zugriffsrechte, die für die Ausführung der jeweiligen Jobrolle erforderlich sind. Systemverantwortliche und Management führen einmal im Quartal Überprüfungen der Nutzerzugriffsrechte durch und bestätigen die gewährten Zugriffsrechte, einschließlich privilegierter Zugriffsrechte. Wenn ein Zugriffsrecht nicht mehr benötigt wird, wird es der Nutzerin oder dem Nutzer entzogen.

Change Management

Der Change Management Standard schreibt die für das Change Management einzuhaltenden Prozesse vor und gibt an, was getan werden muss, um die sichere und geordnete Entwicklung und Bereitstellung von Änderungen an Software und Infrastruktur zu gewährleisten.

Der Change-Management-Prozess schafft die Voraussetzungen dafür, dass vorgeschlagene Änderungen ordnungsgemäß autorisiert, einer Peer Review unterzogen, getestet, implementiert und freigegeben werden und dass der Status der vorgeschlagenen Änderungen dokumentiert und überwacht wird. Auch bei Änderungen wegen eines Notfalls bedarf es einer dokumentierten Genehmigung und automatisierter Tests. Notfalländerungen müssen zudem manuell geprüft werden, wobei diese Prüfung auch nach der Implementierung erfolgen kann.

Lieferkettensicherheit

Die Bereitstellung von Software für Produktionsumgebungen erfolgt über automatisierte CI/CD-Pipelines. Änderungen werden in den dafür vorgesehenen Branches der jeweiligen Repositorys gespeichert. Development-Branches sind für die aktive Entwicklung bestimmt und die Haupt-Branches enthalten produktionsbereiten Code. Änderungen sind versionsverwaltet und bevor sie in die Haupt-Branch gestellt werden, werden sie einer Reihe von automatisierten Tests und Sicherheitsprüfungen unterzogen. Branch-Schutzmaßnahmen sorgen dafür, dass zunächst Tests durchgeführt und bestanden werden müssen, bevor die Änderung ihren Weg in die Haupt-Branch findet. Wenn eine Änderung uneingeschränkt autorisiert worden ist – d. h., die entsprechenden Tests und Sicherheitschecks sind bestanden worden, die Peer Review ist abgeschlossen, die Änderung wurde genehmigt und die Integrationsprüfungen sind erfolgreich verlaufen –, wird die Änderung durch automatisierte Bereitstellungssoftware ganz ohne manuellen Eingriff in die Produktion überführt.

Unser Quellcode ist in einem mit Zugriffskontrollen versehenen und überwachten Versionsverwaltungssystem gespeichert. Die Nutzeraktivität wird mittels Audit-Logs erfasst und es gibt Erkennungsmechanismen, die unerwartete oder verdächtige Änderungen und Build-Prozesse melden. Das Ändern von Code in den einzelnen Repositorys ist nur Nutzer:innen mit genau definierten Jobrollen erlaubt.

Sicheres Entwickeln

SDLC

Die Sicherheitsanforderungen für unseren Systems Development Life Cycle (SDLC) sind im Secure Software Development Framework festgeschrieben. Dieses Framework regelt, wie Elastic-Software jedweder Art sicher konzipiert, entwickelt, bereitgestellt, verfolgt und gepflegt werden kann. Es enthält außerdem Anforderungen zum Schutz unseres Build-Systems und zur Minderung der Risiken von Build-Chain-Kompromittierungen. Build-Systeme bestehen aus Pipelines zur Softwareverteilung, Paketregistrierungsdatenbanken, Artefakt-Repositorys, CI/CD und Systemen für das Quellcodemanagement. Das Secure Software Development Framework untersagt die Nutzung von Produktionsdaten für Testzwecke und in Nicht-Produktions-Systemen. Es schreibt auch eine Trennung von Produktions- und Nicht-Produktions-Umgebungen vor. Zur Bewertung der Segmentierung der Umgebung finden Penetrationstests durch externe Anbieter statt.

Sicheres Design und sichere Architektur

Für die Softwareentwicklung bei Elastic gelten Best Practices für Design und Architektur, die sicherstellen, dass die produzierte Software sowohl konzeptionell („secure by-design“) als auch hinsichtlich der Standardeinstellungen („secure by-default“) sicher ist.

Das Secure Software Development Framework skizziert die Datenschutzanforderungen und Sicherheitsprinzipien, die für alle Design gelten sollen, wie:

- Vertraulichkeit – Daten müssen sowohl bei der Übertragung („in-transit“) als auch im gespeicherten Zustand („at-rest“) vor unbefugter Einsichtnahme oder Offenlegung geschützt sein.
- Integrität – Daten müssen vor unbefugter Erstellung, Änderung oder Löschung geschützt sein.
- Verfügbarkeit – Autorisierte Nutzer:innen müssen auf die für ihre Arbeit erforderlichen Daten zugreifen können und es muss sichergestellt sein, dass etwaige Verfügbarkeits-SLAs eingehalten werden.
- Identifizierung, Authentifizierung und Autorisierung
- Nichtabstreitbarkeit
- Auditing und Logging
- Zugriffssteuerung und „Least-Privilege“-Prinzip
- sichere Kommunikation und Verschlüsselungsstandards
- sichere Standardeinstellungen und Fail-Safe/Fail-Secure

Die Modellierung von Bedrohungen und Überprüfungen der Sicherheitsarchitektur auf die konzeptionelle Einhaltung der erforderlichen Sicherheitsprinzipien sind ebenfalls Bestandteil des Softwareentwicklungsprozesses.

Sicheres Codieren

Als SaaS-Anbieter sind wir uns bewusst, wie wichtig es ist, für die Sicherheit beim Codieren zu sorgen. Daher müssen die entsprechenden Teams und Einzelpersonen einmal jährlich das Secure Software Development Training absolvieren, in dem auf häufige Schwachstellen beim Codieren, wie die „OWASP Top 10“ und die „CWE Top 25“, eingegangen wird. Wenn Änderungen am Quellcode vorgenommen werden, dürfen diese erst nach einer Überprüfung und Genehmigung (mittels eines „Merge-Requests“) durch mindestens eine andere Person als die Autorin oder den Autor der Änderung in die Produktionsumgebung übernommen werden. Änderungen werden auf potenzielle Sicherheitsauswirkungen geprüft. Außerdem finden unabhängige Penetrationstests statt, bei denen die Sicherheit des Codes geprüft wird. Diese konzentrieren sich besonders auf häufig vorkommende

unsichere Praktiken beim Codieren. Wenn bei der Modellierung von Bedrohungen, bei der Sicherheitsüberprüfung oder bei der Überprüfung des Quellcodes mögliche Probleme festgestellt werden, werden diese weiter verfolgt und gemäß des bei der Risikobewertung anhand des Vulnerability Management Standards festgestellten Risikos behoben.

Zur Unterstützung unserer Bemühungen, die Software sicher zu machen und zu halten und die Kunden vor der Ausnutzung von Schwachstellen zu schützen, unterhalten wir auch ein Bug-Bounty-Programm. Wenn Sie mehr darüber erfahren möchten, sehen Sie sich die Informationen zum Programm zur Offenlegung von Schwachstellen (Vulnerability Disclosure Program) im Abschnitt „Schwachstellen- und Patch-Management“ an.

Prüfung von Open-Source- und Drittanbietersoftware

Das Secure Software Development Framework schreibt vor, dass Abhängigkeiten von Open-Source- und Drittanbieterbibliotheken im Code benannt und überwacht werden müssen. Damit wir potenzielle gefährdete Abhängigkeiten identifizieren, finden und beheben können, setzen wir entsprechende Dependency-Management-Software ein.

Schwachstellen- und Patch-Management

Die Grundlage für das Schwachstellenmanagement-Programm bildet unser Vulnerability Management Standard. In ihm werden die Anforderungen für das Prüfen von Elastic-Ressourcen auf Schwachstellen sowie für die Triage, Analyse, Beseitigung und Offenlegung von Schwachstellen festgelegt. Elastic scannt sowohl die Infrastruktur hinter Elastic Cloud als auch die Elastic Cloud-Komponenten auf Schwachstellen und wendet entsprechende Patches an. Diese Prozesse werden unten näher beschrieben.

Schwachstellen- und Patch-Management für die Infrastruktur

Elastic nutzt für das Scannen der eigenen Assets einen kommerziellen Schwachstellen-Scanner. Dieser prüft sämtliche Produktions-Assets. Der externe Anbieter dieser Software hält die verwendeten Regeln fortlaufend auf dem neuesten Stand. Zur Einstufung des Schweregrads der gefundenen Schwachstellen werden die CVSS-Ratings herangezogen und auch die Patching-Fristen richten sich nach den CVSS-Ratings. Schwachstellen mit den Einstufungen „Critical“ und „High“ werden für ein sofortiges Patching oder ein Patching im Rahmen der nächsten geplanten Versionsveröffentlichung priorisiert.

Schwachstellen- und Patch-Management für die Produkte

Wir sorgen dafür, dass unsere Produkte regelmäßig auf Sicherheitsschwachstellen geprüft werden. Zu diesem Zweck lassen wir Penetrationstests durch externe Anbieter durchführen, führen selbst automatisierte und manuelle Codescans und -überprüfungen, OSS-Scans und Segmentierungstests durch und unterhalten ein Programm zur Offenlegung von Schwachstellen. Wenn in einem Elastic-Produkt eine Schwachstelle gefunden wird, wird diese gemäß dem Vulnerability Management Standard evaluiert, um deren Schweregrad festzustellen und einen Abhilfeplan aufzustellen. Sofern erforderlich, veröffentlichen wir ein Elastic Security Advisory (ESA). Das ESA ist eine Benachrichtigung, mit dem Elastic seine Nutzer:innen über Sicherheitsprobleme bei Elastic-Produkten informiert. Elastic weist jeder dieser Advisory-Benachrichtigungen sowohl eine CVE- als auch eine ESA-Kennung zu. Außerdem stellt Elastic eine Zusammenfassung und Informationen zu Abhilfe- und Risikominderungsmaßnahmen zur Verfügung. Neue Advisory-Benachrichtigungen werden im Forum „Security Announcements for the Elastic Stack“ veröffentlicht.

Der Vulnerability Management Standard regelt auch die Veröffentlichung von Offenlegungen. Der Offenlegungsprozess umfasst gegebenenfalls die Veröffentlichung einer neuen Produktversion sowie die Veröffentlichung einer Bekanntmachung auf der Seite mit den Sicherheitsbekanntmachungen. Je nach Art der Schwachstelle können wir auch einzelne Kunden kontaktieren, einen Blogpost veröffentlichen und/oder die CVE-Kennung an MITRE senden.

Kunden können sich mithilfe eines RSS-Feeds über ESAs auf dem Laufenden halten lassen.

Vulnerability Disclosure Program

Elastic unterhält ein öffentliches Programm zur Offenlegung von Schwachstellen (Vulnerability Disclosure Program), über das Security-Expert:innen Schwachstellen melden können, die dann intern geprüft werden. Das Elastic Product Security Team sieht sich die Meldungen an, bewertet das Risiko und kümmert sich um die Beseitigung der Schwachstelle gemäß der Risikobewertung. Wenn Sie sich über unsere Bug-Bounty-Richtlinie informieren oder eine Schwachstelle melden möchten, besuchen Sie das Elastic Bug Bounty Program auf HackerOne.

Third Party Risk Management

Onboarding externer Anbieter

Alle externen Anbieter, einschließlich Unterauftragsverarbeitern, müssen einen gründlichen Onboarding- und Prüfungsprozess durchlaufen. Bei der Evaluierung der Risikoprofile der einzelnen Anbieter werden die vom Anbieter angebotenen Leistungen, die Art der Daten, die der Anbieter verarbeiten soll, das geplante Ausmaß seines Zugriffs auf interne Systeme sowie andere Faktoren für die Kritikalität und das Risikoprofil des Anbieters berücksichtigt.

Je nach Risikoprofil und der Art der zu erbringenden Leistungen wird ein Prüfungs-Workflow ausgeführt. Alle Anbieter, die Zugriff auf vertrauliche Informationen und/oder interne Systeme haben oder kritische Technologieleistungen bereitstellen sollen, müssen zusätzliche Prüfungen durchlaufen. So wird unter anderem geprüft, ob sie die Regeln zur Informationssicherheit, rechtliche Vorgaben und bestehende Datenschutzvorschriften einhalten. Diese zusätzlichen Prüfungen beziehen sich auf die Sicherheitspraktiken, die Sicherheitszertifikationen und das Compliance-Reporting der Anbieter. Es wird berücksichtigt, inwieweit die Anbieter die im Land der Verarbeitung, Speicherung und Übertragung von Daten geltenden Gesetze einhält; bei Bedarf kann Elastic in den Vereinbarungen mit externen Anbietern auch weitere Sicherheitsanforderungen einfordern.

Elastic verfügt auch über einen öffentlich zugänglichen Verhaltenskodex für Anbieter („Vendor Code of Conduct“), in dem die ethischen Anforderungen an Anbieter und Partner verankert sind. Der Verhaltenskodex für Anbieter behandelt unter anderem Fragen des ethischen Geschäftsverhaltens und der Compliance, Anforderungen in Bezug auf den Schutz der Gesundheit und Sicherheit der Mitarbeitenden, Anforderungen in Bezug auf Menschenrechte und arbeitsrechtliche Fragen sowie Umweltschutzanforderungen.

Rezertifizierung externer Anbieter

Für die Rezertifizierung bestehender Anbieter gibt es einen kontinuierlich laufenden „Third Party Information Risk Management“-Prozess. Externe Anbieter werden nach ihrer Risikostufe klassifiziert und das Elastic Information Security Team prüft deren Sicherheitspraktiken gemäß den Anforderungen für die jeweilige Risikostufe.

Die Anbieter von Cloud-Diensten (CSPs), die die Infrastrukturdienste für Elastic Cloud bereitstellen, werden mindestens einmal pro Jahr überprüft und rezertifiziert. Der Rezertifizierungsprozess beinhaltet die Überprüfung des Risikoprofils des Anbieters sowie eine Untersuchung seines Sicherheits- und Compliance-Reportings. So wird sichergestellt, dass die erwarteten Sicherheits- und Compliance-Maßnahmen die von uns in Anspruch genommenen Leistungen angemessen abdecken und dass die Maßnahmen sowohl von ihrer Konzeptionierung als auch von ihrer Umsetzung her wirksam sind.

Bedrohungserkennung

Monitoring und Alerting

Für SIEM-Zwecke verwenden wir Elastic Security. Das ermöglicht es uns, innerhalb kürzester Zeit Erkennungsmechanismen für neu aufkommende Bedrohungen und Angriffsmuster sowie für verdächtige Verhaltensweisen, für das Monitoring der Dateiintegrität und für verbreitete Verhaltensmuster von Malware zu entwickeln und bereitzustellen. Automatische Erkennungsmechanismen ermöglichen die Überwachung unserer Umgebungen in Echtzeit. Verdächtige Anzeichen lösen vorkonfigurierte Alerting-Workflows zur Benachrichtigung der zuständigen Elastic-Mitarbeitenden aus. Das rund um die Uhr arbeitende Threat Detections and Response Team untersucht diese Alerts und leitet bei Bedarf entsprechende Maßnahmen ein.

Zertifizierte und fortlaufend geschulte Mitarbeitende bearbeiten auftretende Sicherheitsereignisse und Incidents gemäß unserem Incident Response Standard und dem Incident Response Plan. Mehr über den Incident-Management-Prozess erfahren Sie im Abschnitt „Incident Response“ dieses Dokuments.

Log-Management und -Aufbewahrung

Für das Log-Management verwenden wir Elasticsearch. Dadurch, dass wir Logdaten aus den verschiedensten Quellen – von Erkennungs-Engines über unsere IaaS-Anbieter bis hin zu Tools für das Schwachstellenmanagement und die Cloud-Admin-Konsole – ingestieren und auf einer zentralen Plattform zusammenführen, können wir robuste Logging-, Auditing- und Forensikfähigkeiten entwickeln.

Um eine Manipulation unserer Logdaten zu verhindern, ist der Zugriff auf sie streng geregelt. Sie können nur von Security-Engineering-Mitarbeitenden bearbeitet werden, die Zugriffsrechte nach dem „Least-Privilege“-Prinzip erhalten haben. Außerdem werden unsere Logging-Systeme

durch automatisierte Erkennungs- und Alerting-Mechanismen, einschließlich Dateiintegritäts-Monitoring, geschützt, die das Threat Detection and Response Team beinahe in Echtzeit über verdächtige Aktivitäten unterrichten

Die Aufbewahrung der Logdaten wird durch unseren Data Retention Standard geregelt, wobei geschäftliche, rechtliche und vertragliche Anforderungen berücksichtigt werden. Wie Sie einen Antrag auf Datenzugriff stellen können, erfahren Sie im Abschnitt „Sicherheit und Schutz der Daten“ dieses Dokuments.

Incident Response

Elastic Information Security hat ein rund um die Uhr arbeitendes Threat Detection and Response Team im Einsatz, das sich ausschließlich um die Bearbeitung von sicherheitsrelevanten Ereignissen und Vorfällen kümmert. Maßgeblich für die Incident-Response-Aktivitäten ist der Incident Response Standard. Dieser behandelt Themen wie die Identifizierung von Ereignissen, den Umgang mit Ereignissen, das Melden von Ereignissen und die Schulungsanforderungen. Außerdem wird in einem separaten Incident Response Plan geregelt, wie die Mitarbeitenden sich auf sicherheitsrelevante Vorfälle vorbereiten sollen, was beim Erkennen, Analysieren, Eindämmen und Bekämpfen von Bedrohungen zu beachten ist, welche Schritte für die Wiederherstellung nach einem Vorfall ausgeführt werden sollen und wie Sicherheitsvorfälle zu melden sind. Die Bearbeitung der Vorfälle liegt in den Händen geschulter Incident-Response-Fachleute, die den Incident Response Plan regelmäßig ausführen und testen. Für jeden Vorfall muss ein dokumentierter After-Action-Report (Abschlussbericht) erstellt werden und es muss festgehalten werden, welche Lehren aus dem Vorfall gezogen wurden.

Sollten wir auf eine Sicherheitsverletzung stoßen oder Kenntnis über einen unbefugten Zugriff auf Systeme oder Daten erlangen, werden die Kunden gemäß den gesetzlichen Vorgaben bzw. den bestehenden vertraglichen Verpflichtungen unverzüglich vom Elastic Legal and Information Security Team benachrichtigt.

Wenn es zu einem sicherheitsrelevanten Vorfall kommt, der einer externen Aufsichts- oder branchenspezifischen Stelle gemeldet werden muss, wird im Elastic Incident Response Plan aufgeführt, welche Berichterstattungspflichten für die jeweilige Situation gelten. Im Plan wird darüber hinaus ein formelles Computer Security Incident Response Team (CSIRT) mit dokumentierten Rollen und Zuständigkeiten benannt, das für eine ordnungsgemäße Kommunikation zwischen den beteiligten Personen sorgen soll.

Zuverlässigkeit

Verfügbarkeit und Status

Für über das Normalmaß hinausgehende SLA-Anforderungen kann auf Elastic Cloud eine High-Availability-Architektur bereitgestellt werden, was auch empfohlen wird. Wenn Sie an einer solchen Lösung interessiert sind, besprechen Sie dies bitte mit Ihrem Account Team. Echtzeit- und historische Daten zur Performance von Elastic können bei Elastic eingesehen werden.

Business Continuity und Disaster Recovery

Neben einem eigenen Business Continuity and Disaster Recovery Standard gibt es bei Elastic auch umfassende Business-Continuity- und Disaster-Recovery-Pläne zur Vorbereitung und Reaktion auf Katastrophenfälle und zur Wiederherstellung der betrieblichen Abläufe nach einem solchen Katastrophenfall.

Elastic agiert seit jeher als global verteiltes Unternehmen. Die Mitarbeitenden werden mit allem ausgestattet, was für die Remote-Arbeit benötigt wird, und bei der Besetzung von Stellen in den global verteilten Teams wird auf geografische Redundanz geachtet. An den Elastic-Standorten gibt es keinerlei Infrastruktur oder IT-Systeme, die die Mitarbeitenden für die Herstellung einer Verbindung zum Unternehmen benötigen oder die für die Bereitstellung von Elastic-Diensten und Unterstützungsleistungen gegenüber den Kunden erforderlich sind.

Elastic verfügt über Disaster-Recovery-Pläne für Elastic Cloud, die mindestens einmal jährlich getestet werden. Die Tests sind jeweils einzigartig und konzentrieren sich jedes Jahr auf einen anderen Bereich, damit wir Wissenslücken und Schwächen bei unseren Fähigkeiten aufdecken können, Systeme und Abläufe technisch wiederherzustellen. Bei jedem Test werden die RTO- und RPO-Werte gemessen und dokumentiert, um sicherzustellen, dass die Wiederherstellung den intern definierten Vorgaben entspricht. Disaster-Recovery-Tests werden gründlich dokumentiert. Dabei werden Szenariodetails aufgezeichnet, es wird eine Zeitleiste der Ereignisse festgehalten und es wird protokolliert, welche Maßnahmen für eine Verbesserung ergriffen werden sollen.

Unabhängige Bewertungen

Penetrationstests

Elastic weiß um die Stärke und Wichtigkeit des Defense-in-Depth-Konzepts, bei dem Dinge wie die Sicherheit des Personals, Lateral Movements, Privilege Escalations und Persistent Threats berücksichtigt werden. Daher beauftragt Elastic mehrere unabhängige Anbieter mit der Durchführung von Penetrationstests auf der Vermittlungs- und der Anwendungsschicht, Segmentierungstests und Prüfungen der Codesicherheit. Penetrationstests finden mindestens einmal pro Jahr statt. Wenn bei diesen Tests Probleme gefunden werden, werden diese unter Berücksichtigung ihrer Kritikalität beseitigt. Die Ergebnisse der Penetrationstests werden auch an die Geschäftsführung übermittelt, damit diese die funktionsbereichsübergreifende Lösung der zugehörigen Probleme und gegebenenfalls die Ergreifung zusätzlicher Vorsorge- und Erkennungsmaßnahmen koordinieren sowie entsprechende Zuständigkeiten festlegen kann. Auf Anfrage werden zusammenfassende Berichte über die durchgeführten Penetrationstests sowie Berichte zum Status der Abhilfemaßnahmen zur Verfügung gestellt.

Zusätzlich zu den von unabhängigen Anbietern durchgeführten Penetrationstests sponsert und unterhält Elastic auch ein formelles Bug-Bounty-Programm zur Offenlegung von Schwachstellen (Vulnerability Disclosure Program). Dieses Programm ermöglicht es Security-Expert:innen, Schwachstellen zu melden, die sie gefunden haben. Das Elastic Product Security Team prüft die Meldungen und sorgt unter Berücksichtigung der Kritikalität der Probleme für deren Beseitigung. Wenn Sie sich über unsere Bug-Bounty-Richtlinie informieren oder eine Schwachstelle melden möchten, besuchen Sie das Elastic Bug Bounty Program auf HackerOne.

Compliance-Vorgaben

Elastic unternimmt große Anstrengungen, Sicherheits- und Compliance-Zertifizierungen und -Attestierungen zu erlangen, die für die Kunden relevant sind. Unsere Kunden in hochgradig regulierten Industriezweigen und Regionen in der ganzen Welt vertrauen uns die Erfüllung ihrer Anforderungen an die Suche, Observability und Sicherheit an und wir nehmen dieses Vertrauen sehr ernst. Eine vollständige Liste aller Zertifizierungen und Attestierungen, die Elastic Cloud bietet, finden Sie unter „Sicherheit unserer Produkte und Services“.

Sicherheit und Schutz der Daten

Elastic ist sich der Rolle bewusst, die die Sicherheit und der Schutz der Kundendaten dafür spielt, dass wir das Vertrauen unserer Kunden gewinnen und aufrechterhalten können. Es ist uns ein Anliegen, unseren Kunden transparent darzulegen, wie wir ihre Daten in Elastic Cloud verarbeiten und vor Offenlegung und Verlust schützen.

Hosten von Daten

Elastic nutzt zur Bereitstellung von Elastic Cloud Anbieter von Cloud-Diensten (CSPs) wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP). Unsere Kunden weltweit können selbst entscheiden, bei welchem der von uns unterstützten CSPs sie ihre Elastic Cloud-Deployments bereitstellen möchten. Dasselbe gilt für die Wahl der Region, in der die Deployments gehostet werden. Dadurch wird für die Einhaltung der Anforderungen an die Datensouveränität gesorgt. Auch Datensicherungen sind so konfiguriert, dass die Sicherungskopien der Kundendaten in der vom Kunden ausgewählten Region bleiben.

Vertragliche Verpflichtungen

Elastic hat im gesamten Unternehmen Prozesse, Organisationsstrukturen und technische Maßnahmen eingeführt, die sicherstellen, dass die globalen Datenschutzgrundsätze eingehalten werden. Dies wird durch die vertraglichen Datenschutzbestimmungen gestützt, die Sie unserem „Customer Data Processing Amendment“ (DPA) für Elastic Cloud entnehmen können.

Um sicherzustellen, dass das DPA jederzeit die geltenden Datenschutzanforderungen erfüllt, wird es regelmäßig überprüft und aktualisiert. Es enthält u. a. die folgenden Bestimmungen:

- Ihre Daten gehören Ihnen. Die Verarbeitung personenbezogener Daten erfolgt nur auf Ihre Anweisungen hin.
- Die Daten, die wir verarbeiten, unterliegen den geltenden gesetzlichen Datenschutzanforderungen.
- Wir haben gemäß unserer vertraglichen Verpflichtungen geeignete technische und organisatorische Maßnahmen ergriffen. Zu diesen Verpflichtungen gehören, sofern zutreffend, die Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission (Standard Contractual Clauses, SCCs).

- Alle Mitarbeitenden, die befugt sind, personenbezogene Daten zu verarbeiten, unterliegen strengen Vertraulichkeitsrichtlinien und -verfahren.
- Kunden werden über Anträge betroffener Personen unterrichtet. Elastic beantwortet solche Ersuchen nicht, ohne zuvor die Einwilligung seitens des Kunden eingeholt zu haben, und unterstützt die Kunden bei der Erfüllung ihrer Pflicht, solche Ersuchen zu beantworten.
- Elastic ist laut SCCs verpflichtet, seine Kunden über Ersuchen von Behörden zu unterrichten, Zugang zu personenbezogenen Kundendaten zu erhalten. Sollte es Elastic aus rechtlichen Gründen verboten sein, diese Daten offenzulegen, ist Elastic gemäß SCCs vertraglich verpflichtet, dieses Verbot anzufechten und sich um eine Aufhebung des Verbots zu bemühen.
- Um sicherzustellen, dass alle Mitarbeitenden, die an der Verarbeitung personenbezogener Daten beteiligt sind, die Vertraulichkeit einhalten, nutzt Elastic Vertraulichkeitsvereinbarungen. Diese Vereinbarungen bleiben auch nach Beendigung des Arbeitsverhältnisses der oder des Angestellten mit Elastic wirksam.
- Die Unterauftragsverarbeiter von Elastic unterliegen denselben Standards und Organisationsanforderungen. Elastic haftet für die Handlungen und Unterlassungen seiner Unterauftragsverarbeiter genau so, als würde Elastic die Dienste selbst erbringen.

Unterauftragsverarbeiter

Elastic nutzt für die Bereitstellung von Elastic Cloud bestimmte externe Dienstleister und interne verbundene Unternehmen, die unter Umständen (als Unterauftragsverarbeiter) personenbezogene Daten von Kunden verarbeiten müssen. Deren Zugang ist ausschließlich auf die Daten beschränkt, die für die Bereitstellung der Leistungen unbedingt erforderlich sind.

Die aktuelle Liste der von Elastic beauftragten externen Unterauftragsverarbeiter finden Sie unter https://www.elastic.co/de/agreements/external_subprocessors. Die internen Unterauftragsverarbeiter sind unter https://www.elastic.co/de/agreements/internal_subprocessors aufgeführt.

Internationale Datenübermittlung und Schrems II

Elastic ist ein globales Unternehmen und kann Daten aus dem EWR und dem Vereinigten Königreich an außereuropäische Mitarbeitende von Elastic und Drittorganisationen übermitteln, die für die Bereitstellung der Dienste des Unternehmens erforderlich sind. Welche Orte dies sind, wird im Abschnitt „Unterauftragsverarbeiter“ oben dargelegt. In solchen Fällen greifen die SCCs, einschließlich des Moduls „Übermittlung von Verantwortlichen an Auftragsverarbeiter“ bei Kunden von Elastic und des Moduls „Übermittlung von Verantwortlichen an Verantwortliche“ bei Unterauftragsverarbeitern von Elastic, sowie robuste ergänzende Maßnahmen. Elastic hat sich die EDSA-Empfehlungen für ergänzende Maßnahmen für die internationale Datenübermittlung nach dem „Schrems II“-Urteil angesehen. Angesichts der praktischen Erfahrungen von Elastic, der geringen Wahrscheinlichkeit eines Interesses seitens der Behörden an den personenbezogenen Daten, die Elastic verarbeitet, sowie der Sicherheitsmaßnahmen, die Elastic zum Schutz der personenbezogenen Daten von Kunden eingeführt hat, ist Elastic nicht der Ansicht, dass die Verarbeitung personenbezogener Daten von Kunden außerhalb Europas durch Elastic ein Risiko für die Rechte Einzelner darstellt, das Elastic davon abhalten müsste, seine Verpflichtungen als „Datenimporteur“ gemäß den SCCs zu erfüllen.

- Interne Analysen und Gutachten externer Berater sind zu dem Schluss gekommen, dass die Datenübermittlungen durch Elastic nicht in den typischen Fokus von Überwachungsgesetzen fallen. Wir bieten außerdem die Umsetzung ergänzender Maßnahmen zum Schutz von übermittelten Daten an.
- Angesichts der Art unserer Leistungen und unserer Datenverarbeitungsaktivitäten sind Ersuchen von Behörden äußerst unwahrscheinlich. Elastic hat bisher kein einziges FISA-, EO12333- oder CLOUD Act-Ersuchen erhalten.
- Die Anwendung der SCCs gilt dem Schutz entsprechender Übermittlungen von Kundendaten. In den Fällen, in denen aus Europa stammende personenbezogene Daten (i) von seinen Kunden unmittelbar an Elastic, (ii) von Elastic gruppenintern zwischen Unternehmen der Elastic-Gruppe oder (iii) von Elastic an externe Unterauftragsverarbeiter übermittelt werden, schließt Elastic SCCs mit diesen Parteien ab.
- Die Daten werden sowohl während der Übermittlung (in-transit) als auch im gespeicherten Zustand (at-rest) verschlüsselt.
- Kunden können festlegen, dass die im Rahmen unserer Dienste verwendeten Anwendungen auf Servern in der EU gehostet werden sollen.
- Elastic arbeitet kontinuierlich daran, seine vertraglichen, technischen und organisatorischen Sicherheitsvorkehrungen zum Schutz von Datenübermittlungen zu bewerten und weiterzuentwickeln.

Ersuchen von Behörden bezüglich des Zugangs zu Daten

Elastic verfügt über Richtlinien und Verfahren, die regeln, wie das Unternehmen auf Behördenersuchen bezüglich des Zugangs zu Kundeninhalten reagiert. Diese Richtlinien und Verfahren berücksichtigen geltende Datenschutzgesetze und die mit Ihnen geschlossene Kundenvereinbarung.

Elastic ist kein geltendes Gesetz bekannt, das seine Fähigkeit beeinträchtigen würde, seine Verpflichtungen in Bezug auf Behördenersuchen zum Zugang zu Daten und erforderliche Offenlegungen zu erfüllen. Elastic wird unter keinen Umständen personenbezogene Daten in einer massiven, unverhältnismäßigen oder willkürlichen Art und Weise herausgeben, die über das hinausgeht, was in einer demokratischen Gesellschaft notwendig ist.

Ungeachtet dessen hat Elastic bisher noch von keiner Behörde ein Ersuchen zum Zugang zu Kundeninhalten erhalten, auch nicht in Bezug auf Section 702 FISA. Uns ist darüber hinaus auch nicht bekannt, dass es jemals zu einem direkten Zugriff auf Kundeninhalte gemäß EO 12333 gekommen wäre. Elastic hat noch nie eine Backdoor oder einen Masterschlüssel für eines seiner Produkte oder Dienste erstellt und hat niemals einer Behörde den ungehinderten oder direkten Zugriff auf seine Server gestattet.

Schutz personenbezogener Daten als Geschäft

Datenschutzerklärung

Mehr darüber, wie Elastic personenbezogene Informationen in Elastic Cloud erfasst, nutzt, offenlegt, übermittelt und speichert erfahren Sie in unserem „Product Privacy Statement“.

Einhaltung geltender Datenschutzvorschriften

Elastic hält sich an die in der Welt geltenden Datenschutzvorschriften, einschließlich DSGVO und CCPA. Wenn Sie als betroffene Person einen Antrag stellen möchten, lesen Sie bitte den Abschnitt „So erreichen Sie uns“ des Dokuments „Allgemeine Datenschutzerklärung“. Weitere Informationen dazu, wie Sie sicherstellen können, dass Ihre Elastic-Deployments DSGVO-konform sind, finden Sie auf unserer Webseite zur Einhaltung der DSGVO bei Elasticsearch und Elastic Stack.

