brabbler

Whitepaper

Sicherheitskonzept der Brabbler AG

22. Juli 2019

Inhalt

Über dieses Dokument 3
Organisatorische Maßnahmen 3
- Unser Security-Team 3
- Schulungen 3
- Physische Sicherheit 4

Entwicklung 4
- Sicherheitsanalysen 4
- Interne Reviews und Audits 4
- Externe Entwicklung 4
- Akademische Kooperation 5

Infrastruktur 5
- Sichere IT-Ausstattung der Mitarbeiter 5
- Hosting 5
- Netzwerksicherheit 5
- Monitoring und Logging 5
- Disaster Recovery und Business Continuity 6

Mitgliedschaften 6
Kontakt 7
Quellen 7

Über dieses Dokument

Wir bei der Brabbler AG haben die Vision einer digitalen Welt, in der Vertraulichkeit und Privatsphäre Realität sind. In der Unternehmen moderne Kommunikationslösungen nutzen können, ohne dabei die Kontrolle über die eigenen Daten aufzugeben. Diese Daten für unsere Kunden und Nutzer zu schützen, ist daher unser wichtigstes Ziel. Dieser Fokus auf Sicherheit spiegelt sich zum einen natürlich in unseren Produkten wider, zum anderen aber auch in den technischen und organisatorischen Maßnahmen, die wir schon ergriffen haben und laufend erweitern.

Organisatorische Maßnahmen

Unser Security-Team

Sicherheit ist bei Brabbler ein fester Bestandteil der Unternehmenskultur, und jeder Mitarbeiter trägt seinen Teil dazu bei.
Darüber hinaus haben wir ein Expertenteam zusammengestellt, das unsere Gesamtstrategie in puncto Informationssicherheit definiert und vorantreibt. Hier ein Überblick über die verschiedenen Rollen und Verantwortlichkeiten:

Security-Team-Mitglied	Aufgaben
Datenschutzbeauftragter	Unser Datenschutzbeauftragter sorgt dafür, dass Brabbler alle geltenden Datenschutzvorschriften, insbesondere nach Vorgabe der Datenschutz-Grundverordnung (DSGVO), umsetzt und einhält. Er berät das Management, ist aber auch Ansprechpartner für alle Mitarbeiter, wenn es um Datenschutzthemen geht. Zudem beantwortet er alle Datenschutzfragen von Kunden, Behörden oder anderen externen Stellen.
Informationssicherheits-beauftragter	Der Sicherheitsbeauftragte definiert Richtlinien, Prozesse und alle weiteren Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Dazu arbeitet er mit verschiedenen Abteilungen im ganzen Unternehmen zusammen.
Enterprise Architects	Unsere beiden Enterprise Architects (einer auf Entwicklungs-, einer auf IT-Operations-Seite) setzen die Business-Strategie von Brabbler in Produktanforderungen um – und Sicherheit ist ein wesentlicher Teil davon. Sie planen, implementieren, prüfen und verbessern die Sicherheitssysteme, unterstützen und betreuen aber auch andere Mitarbeiter in Bezug auf sichere Entwicklungs- und Betriebsstandards.

Schulungen

Die Sensibilisierung der Mitarbeiter ist ein wesentlicher Bestandteil unseres Sicherheitsprogramms. Unser Datenschutzbeauftragter organisiert regelmäßig Datenschutzschulungen für das Management sowie für Mitarbeiter, die Zugang zu personenbezogenen Daten haben. Dabei geht es u. a. um die Anforderungen der DSGVO an die Vertraulichkeit von Kunden- und Mitarbeiterdaten.

Darüber hinaus werden besondere Sicherheitsschulungen für Mitarbeiter unserer Entwicklungsteams angeboten. Diese Schulungen, die meist vom Enterprise Architect durchgeführt werden, drehen sich um Themen wie „Secure Coding“ sowie andere sichere Entwicklungsverfahren (siehe auch Kapitel „Entwicklung“ auf Seite 4).

Physische Sicherheit

Trotz des Einsatzes moderner, softwarebasierter Sicherheitslösungen darf die Sicherheit auf physischer Ebene nicht vernachlässigt werden. Deshalb schützen wir unsere Gebäude mit verschiedenen Maßnahmen:

Elektronische Zutrittskontrollsysteme sichern den Zutritt zu den Gebäuden sowie zu den einzelnen Büros. Bei Erhalt der Schlüsselchips müssen die Mitarbeiter eine Vereinbarung unterzeichnen: Darin sind sowohl Maßnahmen zur sicheren Aufbewahrung des Schlüsselchips festgelegt als auch ein sicherer Prozess, der die Rückgabe des Schlüssels beim Bürowechsel oder Ausscheiden aus dem Unternehmen regelt. Gäste dürfen sich in den Brabbler-Gebäuden nur in Begleitung eines Mitarbeiters aufhalten.

Nachts, an Wochenenden und Feiertagen ist ein Wachmann vor Ort, der das Gebäude erst verlässt, wenn der erste Mitarbeiter am nächsten Arbeitstag eintrifft. Es hält sich also zu jedem Zeitpunkt jemand im Gebäude auf. Darüber hinaus wird die Umgebung der Gebäude videoüberwacht. Der Zutritt zu den Serverräumen ist auf berechtigte Mitarbeiter beschränkt.

Entwicklung

Der erste Schritt zu sicherer Software sind sichere Entwicklungsprozesse. Daher haben wir bei Brabbler eine Reihe von sicheren Entwicklungsverfahren festgelegt, die wir ständig verbessern und erweitern. Hier ein Überblick:

Sicherheitsanalysen

Bei der Planung neuer Entwicklungsprojekte werden die Sicherheitsrisiken vom Enterprise Architect und dem Entwicklungsteam ausführlich analysiert. Als Grundlage dienen Best-Practice-Richtlinien, wie z. B. OWASP Top 10 [1] oder die OWASP Secure Coding Practices [2]. DasErgebnis der Analyse ist eine Liste von Sicherheitsanforderungen, die vor dem Release erfüllt sein müssen.

Interne Reviews und Audits

Der gesamte Code wird in Repositories mit Versionskontrolle eingecheckt. Jede Zeile wird mindestens zwei weiteren Teammitgliedern zum Code-Review vorgelegt. Diese prüfen den Code anhand von internen Review-Leitfäden auf Richtigkeit und Wartbarkeit. Darüber hinaus werden alle Commits einem kontinuierlichen Integrationstest unterzogen.
Der Enterprise Architect führt in regelmäßigen Abständen weitere ausführliche Audits durch, um die Code-Qualität zu überprüfen und ständig zu verbessern.

Externe Entwicklung

Zur Verstärkung unserer internen Entwicklerteams wurde ein externes Team bei Thinslices [3] zusammengestellt. Die externen Teammitglieder sind per VPN an die Brabbler-Entwicklungsumgebung angebunden, haben jedoch keinerlei Zugriff auf Kundendaten. Sie sind zur Verschwiegenheit verpflichtet und dürfen keine projektrelevanten Daten außerhalb der Netzwerke von Thinslices oder Brabbler speichern. Außerdem bestehen umfassende Maßnahmen zum Schutz des Bürogebäudes.

Akademische Kooperation

Um Innovationen vorantreiben, den Wissensaustausch zu fördern und nah dran zu sein an den aktuellen Forschungsergebnissen im Bereich IT-Sicherheit, hat sich die Entwicklungsabteilung der Brabbler AG mit dem Lehrstuhl für Software- und Systemtechnik [4] an der Technischen Universität München[5] zusammengetan. Das derzeit laufende Pilotprojekt ist eine Doktorarbeit über den Schutz der Integrität bei Microservices. Ein entsprechendes Paper wurde bei der Konferenz MSE@STAF 2018 eingereicht und angenommen.
Darüber hinaus sind Masterarbeiten geplant, z. B. über den Einsatz von Public Key Transparency als Schutz gegen Man-in-the-Middle-Angriffe, über die Absicherung von kubectl und über Public Key Tracing Frameworks.

Infrastruktur

Wir möchten, dass Ihre Daten bei uns gut aufgehoben sind – und zwar nicht nur in der App, sondern auch in unserem Netzwerk. Deshalb hier eine Reihe von Maßnahmen, mit denen wir Vertraulichkeit, Integrität und Verfügbarkeit auf unseren Servern und Rechnern sicherstellen.

Sichere IT-Ausstattung der Mitarbeiter

Die Hard- und Software bei Brabbler wird über einen Asset-Management-Prozess verwaltet. Neue Mitarbeiter bekommen eine sicher konfigurierte IT-Ausstattung. Bei Erhalt unterschreiben sie eine Vereinbarung, die sie dazu verpflichtet, verschlüsselte Kommunikationskanäle zu verwenden, wann immer dies möglich ist, und die sichere Konfiguration ihrer Computer auf dem aktuellen Stand zu halten. Soll neue Software angeschafft werden, muss der Bestellwunsch einen Genehmigungsprozess durchlaufen. Dabei nehmen u. a. der Informationssicherheits- und der Datenschutzbeauftragte die Software unter die Lupe. Bei Bedenken können beide ein Veto gegen den Kauf einlegen. Verlässt ein Mitarbeiter das Unternehmen, sorgt ein Off-Boarding-Prozess dafür, dass der Zugriff auf Geräte sofort entfernt und alle Geräte zurückgegeben werden.

Hosting

Unsere Server werden ausschließlich in Deutschland gehostet: Die interne Infrastruktur befindet sich in unserer Zentrale in München. Unsere Websites und E-Mail-Gateways laufen in ISO-27001-zertifizierten Rechenzentren von 1 & 1 IONOS [7] in Karlsruhe und Frankfurt am Main.

Alle Kundendaten liegen in ISO-27001-zertifizierten Rechenzentren in Nürnberg, die von der noris network AG [8] betrieben werden. Um die Verfügbarkeit zu gewährleisten, sind sowohl die Hardware-Systeme als auch die virtuellen Maschinen, auf denen unsere Services laufen, vollständig redundant ausgelegt. Redundante Systeme sind in unterschiedlichen Brandabschnitten untergebracht. Die Server-Hardware bei der noris network AG ist geleast. Für die sichere Entsorgung von Server-Festplatten ist ein Lifecycle-Management-Prozess definiert.

Netzwerksicherheit

Um die Angriffsfläche unserer Server zu minimieren, verwenden wir Best-Practice-Standardeinstellungen und deaktivieren unnötige Software. Der Zugriff auf sensible interne Systeme von außerhalb des Netzwerks unserer Zentrale ist nur über eine VPN-Verbindung möglich. Kundendaten sind nur im Produktionsnetzwerk erlaubt, das zusätzlich durch Intrusion Detection Systems (IDS) und automatische Abwehrmaßnahmen geschützt ist.

Monitoring und Logging

Alle Server werden rund um die Uhr überwacht. Dazu nutzen wir check_MK [9], eine Erweiterung für das Open-Source-Monitoring-System Nagios [10]. Außerhalb der Geschäftszeiten hat immer ein Mitarbeiter des IT-Operations-Teams Rufbereitschaft und erhält bei definierten Monitoring-Events Benachrichtigungen per SMS. Darüber hinaus ist ein Mitglied des Entwicklungsteams als Site Reliability Engineer rund um die Uhr

erreichbar, um bei größeren Problemen mit der Plattform Second-Level-Support zu leisten.
Die Logs unserer Produktionssysteme und Anwendungen werden 5 Tage lang zentral gespeichert und sind schreibgeschützt abrufbar. Darüber hinaus implementieren wir gerade die Erfassung von Systemprotokollen, insbesondere zur Erstellung eines Audit-Trails für administrative Tätigkeiten.

Disaster Recovery und Business Continuity

Um für den Ernstfall gewappnet zu sein, setzen wir auf volle Redundanz der Produktionssysteme (siehe Kapitel „Hosting“ auf Seite 5) sowie auf eine effiziente Backup-Strategie, bei der die Konfigurationen alle Systeme inhouse gesichert werden. Damit können wir die Systeme in einem Zeitraum neu installieren, der dem eines Restores aus einem herkömmlichen Backup entspricht. Daten, die im Ernstfall unbedingt erforderlich sind, werden einmal wöchentlich in einem ISO-27001-zertifizierten Rechenzentrum in Nürnberg gesichert, das von Hetzner Online [11] betrieben wird.
Um die Sicherheit der Live-Daten unserer Kunden zu gewährleisten, verwenden wir auf unseren Systemen das Dateisystem Ceph [12], das jedes Objekt 3-mal repliziert. Ceph kann den Ausfall jeder Komponente abfangen und verfügt über Selbstheilungsfunktionen, d. h., es kann zerstörte Daten aus Replikaten auf anderen Speichermedien wiederherstellen.

Mitgliedschaften

Die folgenden Mitgliedschaften demonstrieren unsere Bemühungen auf dem Gebiet der Informationssicherheit. Weitere Mitgliedschaften sind bereits beantragt.

SecurITy made in Germany	Als Mitglied von **SecurITy made in Germany** [13] verpflichten wir uns zur Entwicklung vertrauenswürdiger IT-Sicherheitslösungen in Deutschland - ohne Backdoor und im Einklang mit dem deutschen Datenschutzgesetz.
Teilnehmer der Allianz für Cyber-Sicherheit	Als Mitglied der **Allianz für Cyber-Sicherheit** [14] kooperieren wir mit anderen Unternehmen, Behörden und Forschungseinrichtungen, um die Cyber-Sicherheit in Deutschland zu stärken.
Software Bundesverband IT-Mittelstand Made in Germany 100% Service Quality Future	Als Mitglied des Bundesverbands IT-Mittelstand wurde uns das Siegel **Software made in Germany** [15] verliehen. Dies zeigt, dass wir ein deutsches Unternehmen sind und alle wesentlichen Herstellungsschritte sowie die Qualitätssicherung hier stattfinden. Darüber hinaus dient das Siegel als Nachweis für die Zukunftssicherheit unserer Produkte.

Kontakt

Informationssicherheit ist kein Projekt, sondern ein Prozess. Besonders in dieser frühen Entwicklungsphase arbeiten wir laufend daran, nicht nur unser Produkt, sondern auch unser firmenweites Sicherheitskonzept zu verbessern. Wenn Sie Fragen zu unseren Sicherheitsmaßnahmen haben, wenden Sie sich bitte an:

Brabbler Secure Message and Data Exchange AG
– IT-Sicherheit –
Ria-Burkei-Straße 26
81249 München

E-Mail: sicherheit@brabbler.ag

Quellen

[1] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[2] https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
[3] https://www.thinslices.com
[4] https://www22.in.tum.de/de/startseite/
[5] https://www.tum.de/nc/startseite/
[6] https://mse-staf18.fbk.eu
[7] https://www.ionos.de/
[8] https://www.noris.de/
[9] https://checkmk.de/
[10] https://www.nagios.org
[11] https://www.hetzner.de
[12] https://ceph.com/ceph-storage/file-system/
[13] https://www.teletrust.de/itsmig/
[14] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html
[15] http://www.software-made-in-germany.org