brabbler

Whitepaper

# Brabbler AG Security Concept

12 July 2018

# Contents

# About this document

We at Brabbler AG share the vision of a digital world where privacy and confidentiality have become reality. Where organizations can harness modern ways of working without giving up control of their data. Thus, protecting the data that our clients and users entrust to us is our top priority. This focus on security is reflected, of course, in our products, but also in the efforts we've taken – and will continue to expand – as a company on the technical and organizational levels.

# Organizational security

## Our security team

At Brabbler, security is part of our company culture, and every employee contributes to it.
In addition, we've installed a team of experts that are in charge of defining and driving forward our overall information security strategy. Here's an overview of their individual roles and responsibilities:

| Security team member | Job |
|---|---|
| **Data Protection Officer** | Our Data Protection Officer ensures that Brabbler AG implements and complies with applicable privacy regulations, especially the General Data Protection Regulation (GDPR). He's a consultant to the management, but also available for all staff members in case of privacy-related questions. Besides, he answers privacy-related requests from customers, authorities, or other external parties. |
| **Chief Information Security Officer** | The Chief Information Security Officer defines and implements policies, processes, and other controls to ensure confidentiality, integrity, and availability of information. To do that, he works together with various departments throughout the Brabbler organization. |
| **Enterprise Architects** | Our two Enterprise Architects (one on the development, one on the operations side) translate business strategy into product requirements – and security forms a major part of these. They plan, implement, check, and improve the security systems at Brabbler, but also support and mentor other staff members with regard to secure development and operating practices and standards. |

## Trainings

Raising awareness among employees is a key element of our security program. Our Data Protection Officer conducts regular privacy trainings for the management as well as for staff members with access to personal data. Topics include, among other things, requirements of the GDPR with regard to the privacy of customer and employee data.

In addition, we provide specific security trainings for members of our development teams. These sessions are usually conducted by the Enterprise Architect and cover topics such as secure coding and other secure development practices (see also chapter "Development", page 4).

### Physical security

Despite the use of sophisticated software-based security products, the importance of security on a physical level shouldn't be overlooked. That's why we protect our buildings with a variety of controls:

We have electronic access control systems in place that protect access to the buildings as well as to the individual offices. When receiving their key tags, employees must sign an agreement: It stipulates security measures to be taken by the employee to keep the key tag safe, and defines a secure process of returning the key when moving office or leaving the company. Guests don't have unescorted access to the Brabbler buildings.

At night, during weekends, and on bank holidays, a security guard is present and doesn't leave until the first employee arrives on the next workday. This ensures that there's someone in the building at all times. In addition, we have video monitoring systems in place covering the building surroundings. Access to server rooms is limited to entitled staff.

## Development

The first step to building secure software products is to introduce security into the development process. At Brabbler, we've defined a set of secure development practices that we are constantly refining. Here's an overview of what we do:

### Security assessments

When new software development projects are planned, the development team, led by the Enterprise Architect, thoroughly assesses the security risks involved. This process is based on best-practice guidelines such as OWASP Top 10 [1] or OWASP Secure Coding Practices [2]. The result of this assessment is a list of security requirements to be fulfilled before the change may be released.

### Internal reviews and audits

All code is checked into version-controlled repositories. Every line of code committed undergoes code review by at least two other team members. They check the code for correctness and maintainability based on internal review guidelines. In addition, all commits are subject to continuous integration testing.
In regular intervals, the Enterprise Architect conducts further in-depth audits to check and constantly increase code quality.

### External penetration tests

Besides our internal auditing processes, we also have our code reviewed by external experts: The development of the ginlo beta version was largely accompanied by external penetration testing to detect and eliminate vulnerabilities in an early phase. This code still forms the basis for the current ginlo @work app and is constantly enhanced. Further penetration tests are conducted on a regular basis.

### External development

Our internal development teams are reinforced by an external team at Thinslices [3]. External team members can access the Brabbler development environment via VPN, but they don't have access to any customer data. They are obliged to follow a confidentiality agreement and must not store any project-relevant data outside Thinslices' or Brabbler's networks. Besides, they have comprehensive physical security measures in place to protect their office building.

## Academic cooperation

To drive innovation, promote knowledge transfer, and gain access to latest research results in the field of IT security, the Brabbler AG development department has teamed up with the Chair of Software and Systems Engineering [4] at Technical University of Munich [5]. The pilot project we're conducting is a PhD thesis on integrity protection in microservices. A paper was submitted and accepted for the MSE@STAF 2018 conference [6].
Further cooperations with master students are planned, e.g. on the usage of public key transparency to mitigate man-in-the-middle attacks, on securing kubectl, and on public key tracing frameworks.

# Infrastructure

We want your data to be safe – not only within the app, but also when stored in our network. Here's a list of steps we take to ensure confidentiality, integrity, and availability on our servers and workstations.

## Workplace security

Hardware and software at Brabbler is managed through an Asset Management process. New hires are provided with securely configured equipment. When receiving it, they sign an agreement that obliges them to use encrypted means of communication wherever possible and to keep the secure configuration of their computers up-to-date. Any requests for new tools must go through an approval process in which, amongst others, the Chief Information Security and Data Protection Officers evaluate the tool in question and can veto the purchase. When an employee leaves the company, a defined off-boarding process ensures that access to devices is immediately removed, and all equipment is returned.

## Hosting

Our servers are hosted exclusively in Germany: The internal infrastructure is completely located in our headquarters in Munich. Our websites and e-mail gateways run in ISO 27001 certified data centers by ProfitBricks [7] in Karlsruhe and Frankfurt/Main.

All customer data is stored in ISO 27001 certified data centers operated by PlusServer [8] in Cologne. To ensure availability, both the hardware systems and the virtual machines running our services are fully redundant; redundant systems are located in separate sections of the building. The server hardware at PlusServer is leased. A lifecycle management process defines the secure disposal of server disks.

## Network security

To minimize the attack surface of our servers, we use best-practice default settings and disable unnecessary software. Access to sensitive internal systems from outside our headquarters' network is only possible via a VPN connection. Customer data is only permitted on the production network, which is additionally protected using intrusion detection systems (IDS) and automatic countermeasures.

## Monitoring and logging

All our servers are monitored 24/7 using check_MK [9], an extension for the Nagios open-source monitoring system [10]. Outside working hours, one member of the operations team is always on stand-by and receives SMS notifications for defined monitoring events. In addition, one member of the development team is available 24/7 as a Site Reliability Engineer, providing second-level support in case of major platform issues. The logs of our production systems and applications are stored centrally in read-only format for 5 days. In addition, we're currently implementing the collection of system logs, especially to provide an audit trail for administrative activities.

### Disaster recovery and business continuity

To be well-equipped for worst-case scenarios, we rely on full redundancy of production systems (see chapter “Hosting”, page 5) as well as on an efficient configuration backup strategy that we follow for all our systems: The configuration secured in-house allows us to reinstall systems in a time frame equivalent to the restore from a traditional backup. Data that is essential in the event of a disaster is backed up once a week to a ISO 27001 certified data center in Nuremberg operated by Hetzner Online [11].
To ensure the security of our customers’ live data, the file system Ceph [12] deployed on our systems replicates every object 3 times. It can catch the failure of any component and has self-healing features, i.e. it can restore destroyed data from replicas to other storage media.

## Product design

### Security by design

In our solution ginlo @work, we rely on full encryption of all content at any time. This means that content is not only end-to-end encrypted when it’s transmitted, but also when stored locally on a device. Messages can be decrypted by the conversation participants as well as by the team administrator – thus, organizations stay in full control of their data at any time. No one else has access - neither do we as the provider.
For a detailed overview of our encryption concept as well as other security controls implemented in our solution, please refer to the *ginlo @work Security Whitepaper*.

### Privacy by design

We want to help you keep your data confidential, and data minimization is one part of this. We only collect and store the data necessary to provide you with a good service. For an overview of the data we store about our customers, and what this data is used for, please refer to the *ginlo @work Privacy Whitepaper*.

## Memberships

The following memberships demonstrate our efforts in the field of information security. Additional memberships are currently pending.

| | |
|---|---|
| SecurITy made in Germany | As a member of **SecurITy made in Germany** [13] we commit to provide trustworthy IT security solutions developed in Germany, without backdoors and in accordance with German data protection law. |
| Teilnehmer der Allianz für Cyber-Sicherheit | As a member of **Allianz für Cyber-Sicherheit** [14], we cooperate with other companies, authorities, as well as research institutions to strengthen cyber security in Germany. |
| Software Bundesverband IT-Mittelstand Made in Germany 100% Service Quality Future | As a member of Bundesverband IT-Mittelstand, we’ve received the **Software made in Germany** quality seal [15], which certifies that our company is based in Germany and all essential production steps as well as quality assurance take place here. Besides, the seal confirms the sustainability of our products. |

## Contact

Information security is a process, not a project. Especially in this early phase, we're constantly improving not only our product, but also our security concept as a company. If you have questions about the actions we take, please get in touch with us:

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

E-mail: security@brabbler.ag

## References

[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/en/homepage/
[5] https://www.tum.de/nc/en/homepage/
[6] https://mse-staf18.fbk.eu
[7] https://www.profitbricks.de/en/
[8] https://www.plusserver.com/en/en
[9] https://mathias-kettner.com/check_mk.html
[10] https://www.nagios.org
[11] https://www.hetzner.com
[12] https://ceph.com/ceph-storage/file-system/
[13] https://www.teletrust.de/en/itsmig/
[14] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html
[15] http://www.software-made-in-germany.org/english-summary/