Systems, Safety and Encryption

February 16, 2016

Abstract

This document discusses the systems and safety procedures at Bullsender ApS

Handled with Care by Experts

Bullsender leverages the expertise and top notch hardware to ensure that the integrity of your data is kept intact. At Bullsender, we recognize that remaining secure involves active monitoring, constant improvements and building on the knowledge that others have worked to discover. Whether it be through hardware, software and networking analysis from our system administrators, or the generous open source software we use - we try to incorporate as many tools as possible to ensure Bullsender remains a secure and trustworthy service. Our servers - from power supplies to the internet connection to the air purifying systems - operate at full redundancy. Our systems are engineered to stay up even if multiple servers fail.

Top Notch Data Center

Bullsender's servers are managed in-house and located in a SOC 2, Type II audited facility that is located in the France. The data center includes high-end surveillance equipment, security guards, visitor logs and passcards/biometric recognition. With fully redundant IP connections, independent connections to T1 access providers, redundant external and internal power sup-plies, daily security scans and encrypted offsite backups, you can rest assured that we are doing everything we can protect your valuable data.

Encouraging the Best Coding Practices

In addition to implementing features that increase security, we have to maintain best practices on the backend to ensure your account remains secure. We monitor sessions to restrict access of your account appropriately, and have constructed Bullsender in a way that every account is isolated. Safeguards are in place to try and detect common attacks such as SQL injection and cross site scripting. Most importantly, we actively review our code for potential security concerns (in addition to evaluating all user feedback) so that we can address any issues as quickly as they arise. Also, remember that we are all bound to our privacy statement, which will ensure your data is not misused.

Secure Data Transfer and Storage

We Strongly enforce the secure collection of data. Forms will be served across a protected, 256-bit SSL connection that encrypts the data before it is sent to our servers. SSL ensures that any wrong-doer who may be listening in to your network traffic is not able to actually read the data being submitted. Whenever your data is in transit between you and us, everything is encrypted,and sent using HTTPS. Any files which you upload to us are stored and are encrypted at rest.
Our backups of your data are secured using a custom salt and encrypt procedure even before it is sent to our backup servers.

We Have Backups of Our Backups

Disasters happen, so being prepared for them is critical for happy data collection. You can rest easy when you store your data with Bullsender, because we are consistently replicating (backing up in real time) your data on site to another server. Additionally, we take full snapshots of your data every 24 hours and store them on site for a week. Additionally we store weekly snapshot for 3 months. Just as we have backups of your data, we also have lots of redundancy across our core infrastructure.

How We Secure the Network

We have an outside routing layer that provides basic filtering to handle and manage any potential denial of service attacks. All network traffic then has to pass through one of our firewalls, which are heavily locked down and allow only specific services to be made publicly available. Additionally, we perform periodical scans, to look for any potential vulnerabilities in our network or publicly accessible software. In regards to employees, we force outside access to the servers to use a 128-bit encrypted connection along with a strong password strength.