Security Whitepaper for myTobiiDynavox®

myTobiiDynavox® is a cloud-based storage system that provides critical day-to-day backup, storage, restoration and sharing services to Tobii Dynavox device users, for our communications app users, and care givers and prospective clients who need to store or share page sets, bank messages, or to learn about or buy Tobii Dynavox products. Learn how myTobiiDynavox has been built to deliver reliable and secure service within existing networks and security infrastructure.

Introduction

myTobiiDynavox is an online, integrated system that allows users to backup, store, share and restore files across multiple platforms, including Tobii Dynavox speech generating devices, iPad®, and Windows® tablet PCs. The myTobiiDynavox site fills a pivotal role in the Tobii Dynavox communication solution "ecosystem" because it can meet a wide variety of needs for the users of speech generating devices and for those that support them.

myTobiiDynavox functionality includes:

- Online storage and management of communication pagesets and subsets
- Access to print and video resources that aid in the configuration and use of Tobii Dynavox hardware and software
- Instructor and caregiver implementation supports
- Software downloads for editing, Windows, and other utilities
- Sharing of communication pages and pagesets between accounts
- Recorded message banking and transcription

myTobiiDynavox is hosted entirely by Tobii Dynavox. The service is composed of three main components:

- Information about Tobii Dynavox devices and software, a page set sharing facility, and myTobiiDynavox
- The myTobiiDynavox Portal where each customer is provided with a unique login area for access to their account. A user simply visits the secure site, enters a username & password , and then receives access to their particular user account.
- Access to search for and find software and supporting documentation, and search for existing Knowledgebase articles specific to the Tobii Dynavox devices and software.

Protecting the integrity and the privacy of data associated with customers is a high priority. In addition, to ensure low total cost of implementation (TCI), online support systems must integrate

smoothly with a variety of customers' existing security infrastructure and require little IT support. myTobiiDynavox, was developed with both goals in mind. Secure from the ground up, myTobiiDynavox uses an ASP model designed expressly to ensure robust and secure operation while integrating seamlessly with your organization's existing network and security infrastructure.

Secure facility

myTobiiDynavox software, communication and database servers are hosted by Microsoft Azure cloud services in a highly-secured Tier 1 data center. Physical access to servers is restricted. The entire site sits in a locked cage that is monitored by security cameras to prevent unauthorized access.

Additional information on Microsoft physical security can be found at https://azure.microsoft.com/en-us/blog/azure-layered-approach-to-physical-security/

Secure platform

myTobiiDynavox runs on hardened Windows servers with the latest security patches installed. Servers are owned, operated, and hosted by the Microsoft Azure service. The myTobiiDynavox servers are configured to watch for denial of service (DoS) attacks and to log denied connections. Multi-layer perimeter security is provided by a pair of firewalls: one between the Internet and Web servers, another between the Web servers and back-end databases. The system is fully PCI compliant.

Scalable and reliable infrastructure

The myTobiiDynavox infrastructure is both robust and secure. Redundant routers, load balancers, server clusters and backup systems are used to ensure high availability. For scalability and reliability, load balancers transparently distribute incoming requests among myTobiiDynavox servers. For optimal performance, the system load balances the client/server sessions across distributed communication servers hosted in central Canada.

Protecting customer privacy

Tobii Dynavox understands that customers are concerned about privacy. We have a strong privacy policy that prohibits unauthorized disclosure of user or enterprise customer information to any third party. This policy identifies the information gathered, how it is used, with whom it is shared and the customer's ability to control the dissemination of information. The Tobii Privacy Policy can be found at https://www.tobii.com/group/privacy-policy.

Protecting user data

User data on myTobiiDynavox is stored in proprietary, compressed file formats that further protect personal information from being visible to the casual observer. All user data stored by myTobiiDynavox is protected at rest using 256-bit AES encryption provided by the Azure cloud service.

User email addresses

Each account user must include a valid email address to successfully use the myTobiiDynavox system. Each account must use a unique email address and be verified by the owner.

Disclosure of customer information

To deliver the myTobiiDynavox service, Tobii Dynavox must collect certain user information, including first/last name, email address and account-level passwords. Unless expressly authorized, Tobii Dynavox will not disclose this confidential information to any third party or use this information in any manner other than to deliver agreed services. Tobii Dynavox may send service update messages to its users at the email addresses they provided when creating an account.

Even when myTobiiDynavox is accessed from a public PC, no personal data is left behind that could pose a privacy threat. myTobiiDynavox uses an optional cookie to remember a user's username if they explicitly request that using the "remember me" option on login. This cookie contains only the username, but does not contain any personally identifiable information or passwords. Users can block this cookie if desired. After a session ends, browser history indicates that myTobiiDynavox was accessed – but information in the history cannot be used to access the account.

Access to customer information

Tobii Dynavox staff members are the only individuals with access to Tobii Dynavox servers – limited access is granted on a need-to-know basis for the express purpose of customer support. Tobii Dynavox developers do not have access to data stored on Tobii Dynavox's production servers.

Tobii Dynavox tracks domain names and browser types for traffic management. However, this data is gathered in the aggregate and is never correlated with an individual user.

Firewall compatibility

myTobiiDynavox is firewall friendly. It generates only outgoing HTTPS/TCP to ports 8080, 443 and/or 8200. Because most firewalls are already configured to permit outgoing Web traffic, you do not have to bypass or compromise your district or location firewall.

Protecting confidential data

myTobiiDynavox uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. All traffic between the user's browser and the server is protected with end-to-end 128-bit AES encryption.

Advanced encryption

myTobiiDynavox supports 256-bit Advanced Encryption Standard (AES) in Counter Mode (CTR).   Modern browsers and operating systems will automatically select 256-bit encryption for the user. In early 2001, after an extensive four-year evaluation process, the National Institute of Standards and Technology (NIST) selected AES as a successor to DES. Originally known as Rijndael, AES was selected because of its computational efficiency, modest memory requirements, flexibility, simplicity, and of course, security. AES is now the U.S. government's designated cipher for protecting sensitive information. Through industry-standard encryption methods, myTobiiDynavox can help an organization implement strong security policies and conform to district privacy mandates.

Password Protection

Any system that allows users to login can be compromised by using weak passwords that can easily be guessed, or by sharing passwords. myTobiiDynavox enforces a minimum password length of 8 characters, and it does display password strength when users are creating or changing their passwords. Unsecure passwords are not permitted.

Password Recovery

If a user forgets their password, the login screen has a "Forgot Password" link that will ask for their email address. If the address matches the one we have in the system, an email will be sent with a link to allow the user to reset their password.

Inactivity time-outs

If a user walks away from their laptop or desktop computer, or switches away from the myTobiiDynavox site without logging out, myTobiiDynavox addresses this issue by applying inactivity time-outs. Users are automatically logged out of the website or app if their SSL connection is inactive for several minutes.

Conclusion

Tobii Dynavox's approach to security and privacy is simple: Start with a secure hosted service and operational practices that preserve customer privacy. Protect data connections with authentication and state-of-the-art encryption to keep traffic safe. Integrate this solution seamlessly with each district's existing network and security infrastructure. Provide flexible

administrative controls for user management. The end result: myTobiiDynavox is a robust, secure education management and delivery system with low total cost of implementation (TCI).

Tobii Dynavox

Product information: www.myTobiiDynavox.com

For more information on Tobii Dynavox please visit www.TobiiDynavox.com

About Tobii Dynavox

Tobii Dynavox, part of the Tobii Group [STO: TOBII], is the leading provider of touch and eye tracking based assistive technology hardware and software for those with communication and mobility challenges. We have helped thousands of individuals with disabilities such as aphasia, autism, cerebral palsy, ALS, muscular dystrophy, Rett syndrome and spinal cord injury lead fuller and richer lives. Tobii Dynavox stands at the forefront of assistive technology and special education, delivering the most advanced, effective and empowering communication and computer access tools available.