dydx.software

10-09-2019

Attention: Springbok Relief Incorporated

I am writing to address some of your questions regarding the operational and security standards upheld by Dydx Software, it's third parties and ultimately the Springbok Relief Incorporated Wiki. The aim of this document is to help ease any concerns about the Wiki's usage in both private companies and government organisations alike.

The following document outlines a few key details about the Wiki's implementation and infrastructure.

0423 596 714 kyle@dydx.software www.dydx.software

1) Hosting

In terms of the physical servers, Dydx Software hosts all client's software on Amazon Web Services (AWS). Hosting is split between various Sydney data centres for latency, redundancy and data protection purposes.

For peace of mind, AWS hosts many large enterprises such as Suncorp Bank, Commonwealth Bank, Netflix, McDonalds as well as many other government organisations such as NASA, FDA, US Department of State and UK Ministry of Justice.

The following are links to various case studies by AWS customers for your interest:
https://aws.amazon.com/solutions/case-studies/enterprise/
https://aws.amazon.com/solutions/case-studies/government-education/

Furthermore AWS has been awarded PROTECTED Certification by The Australian Cyber Security Centre (ACSC) - This is currently the highest data security certification in Australia.
https://awsinsight.com.au/insight/aws-protected-status/

Other notable AWS compliance certifications include CSA, PCI DSS Level 1, SOC (1,2,3), ISO 9001, ISO 27001, 27017, 27018, IRAP and many others. The following link details this further:
https://aws.amazon.com/compliance/programs/

2) Physical Infrastructure Access

Due to AWS's incredibly strict data centre practices and non-public data centre locations, it is near impossible for attackers to gain access to the physical servers and underlaying networking infrastructure. Access to facilities is heavily monitored, logged and controlled.

This alone is one major reason Dydx exclusively hosts with large cloud providers – we simply don't trust small independent, third party hosting services.

For more detailed info see the following link:
https://aws.amazon.com/compliance/data-center/controls/

3) Account Access

With physical server access being impossible, Dydx then accepts the responsibility for implementing best practices to assure our digital access is protected.

For the sake of brevity, we employ strict access control policies which ensure no developer has access to production systems unless it is *absolutely* necessary. Moreover servers are not accessible via public endpoints (Isolated from public internet) and all ports on a network and machine level are locked down by default.

Therefore all access has to be manually granted by an admin on a network and AWS account level.

In the rare event that a developer requires machine access, an admin would first need to authorise network access to a specific AWS resource via a unique and refreshed dedicated IP, for a pre-defined purpose and timeframe.

This said, production level access is usually unnecessary as all deployments / updates go through a rigorous testing process, to a point where updates can be reliably deployed by software tools without the need for human interaction.

We also have monitoring in place to log user access and automatically alert *and* shut down access in the event of human error, or if odd behaviour is detected on machines, databases, the network or an even on an AWS account level.

With regards to AWS account access, we take full advantage of 2 factor authentication, password rotation, strict access control policies and also perform regular account access audits.

4) Data Transmission

As briefly mentioned above, all server access/communication is strictly controlled at a network level, therefore software traffic is also protected at this level.

In the case of the Wiki, all server traffic is fully encrypted and forced over HTTPS. Therefore no personal information is ever transmitted via plain text and thus cannot be intercepted and decoded on insecure networks. (E.g. Public Wifi)

Furthermore, Our SSL/TLS certification is handled by AWS and is thus protected against accidental expiry, certificate leaks or similar.

Moreover during transmission, we also take great care to ensure logging tools do not accidentally expose any private information obtained from a web request. (E.g We ensure email addresses etc are redacted in logs)

5) Data Storage

With regards to data storage, Dydx prefers to use a range of AWS storage methods for simplicity our side as well as for the obvious cost and security benefits associated with managed platforms.

For database storage, the Wiki uses Amazon Relational Database System (RDS).
This means all data is encrypted at rest and lives on private, single tenant databases. These databases are also isolated from public internet at the network level.

For file storage, the Wiki uses Amazon Simple Storage System (S3)
This ensures data does not live on the production servers and can be treated and audited independently. As a best practice, all files are stored in private “buckets” which are not accessible via the public internet without pre-authorization via AWS servers.
These file requests are time bound and are logged for obscure access detection / automatic lockdown.

The same resource / account access policies mentioned in the above “Account Access” section are also applied here. – Developers don’t get production data access.

6) Web Technologies

With the wiki being deliberately private & secure by nature, we do not use tracking methods such as cookies, ads or other tools as used by commercial websites. – There is no need to re-engage or remarket to our users.

Therefore you should rest assured that there is no spam, ads, clickbait or other malicious tools / downloads used to generate revenue or prolong user engagement.

The wiki is a plain HTML & JavaScript application sitting on secure servers, with the sole purpose of education and information dispersal.

By comparison, accessing any other public website poses far greater risk to an organisation, as the source and contents of its data is potentially unknown, unmanaged and open for manipulation by any third party.

The reality is that there is a “standard” level of risk when accessing any website, therefore operating systems, web-browsers and IT departments employ many protection practices by default.

Therefore if any business / government allows public internet access, there is no reason for them to view the wiki any differently. Web & Infrastructure standards exist for a reason, and Dydx Software exists because we adhere to these.

dydx.software

In summary, I would like to personally reassure your IT team, staff and wiki readers that any concerns about personal or organisational privacy are ill-founded and need not hinder access to the Wiki and the vital information held within.

I can assure you, accessing any public website holds far greater risk than accessing this intentionally private and secure wiki.

Again, I am more than happy to discuss this further if need be.

Kind regards,

Kyle Tully
Software Engineer

0423 596 714 kyle@dydx.software www.dydx.software