RESOURCE CENTER

Wie End-to-End-Verschlüsselung den Weg für Zero Knowledge ebnet – Whitepaper

Bitwarden ermöglicht Passwortverwaltung mit Zero-Knowledge-Verschlüsselung

Get the full interactive view at https://bitwarden.com/de-de/resources/zero-knowledge-encryption-white-paper/

bitwarden

As more of our daily and professional lives move online, both personal and company security depends on all of us. Cyber attacks and data breaches unfortunately continue, with password management often cited as an easy step to mitigate risk.

But how can you trust a company to keep all of your secrets secret? The answer lies in end-to-end encryption, which lays the groundwork for applications with 'zero knowledge' architectures.

In a recent article on Tech Radar, author Christian Rigg noted,

> Zero knowledge refers to policies and architecture that eliminate the possibility for a password manager to access your password.

While this is a perfect explanation of zero knowledge for a broad audience, security experts will differ in the interpretation of zero knowledge. We know we want zero knowledge in terms of safely handling encrypted passwords with password managers, but what exactly does that mean?

Beginnen Sie mit einer starken Ende-zu-Ende-Verschlüssel

Die Grundlage einer sicheren Architektur beginnt mit der Verschlüsselung, insbesondere der Ende-zu-Ende-Verschlüsselung. Bei Bitwarden verschlüsseln wir Ihre sensiblen Daten sofort, sobald Sie sie in einen Bitwarden-Client eingeben. Bevor die Daten auf Ihrem Gerät gespeichert werden, werden sie verschlüsselt. Es gibt keine unverschlüsselten Vault-Daten, außer wenn Sie die Kontrolle haben und die Informationen in einem Bitwarden-Client anzeigen, in dem Sie Ihre E-Mail-Adresse und Ihr Master-Passwort eingegeben haben.

Von dort aus bleiben alle Vault-Daten verschlüsselt, wenn sie an die Bitwarden Cloud oder einen selbst gehosteten Bitwarden-Server gesendet werden. Beim Synchronisieren der Daten mit anderen Clients bleibt sie verschlüsselt, bis die eindeutige E-Mail-Adresse und das Master-Passwort erneut eingegeben werden.

Das bedeutet, dass Bitwarden als Unternehmen Ihre Passwörter **nicht sehen kann**, sie bleiben Ende-zu-Ende mit Ihrer individuellen E-Mail und Ihrem Master-Passwort verschlüsselt. Wir speichern Ihr Master-Passwort niemals und können nicht darauf zugreifen.

Für Vault-Daten verwendet Bitwarden eine AES-256-Bit-Verschlüsselung, einen Industriestandard, der als unzerbrechlich gilt. Für Ihr Master-Passwort wird PBKDF2 SHA-256 verwendet, um den Schlüssel abzuleiten, der Ihre Vault-Daten verschlüsselt. Um mehr über die Sicherheit von Bitwarden zu erfahren, besuchen Sie bitte unsere Sicherheits-FAQ.

Verständlicherweise ist das wichtige Detail der Ende-zu-Ende-Verschlüsselung der Schlüssel zur Entschlüsselung. Solange dies **nur** beim Endbenutzer bleibt, kann eine Lösung zu einer Zero Knowledge-Architektur führen.

Es gibt Fälle, in denen Software- und Dienstanbieter die Verschlüsselung fördern, aber den Schlüssel behalten. Diese Fälle gelten aus unserer Sicht nicht als Nullwissen, da die Software- und Dienstleister technisch in der Lage sind, die Daten zu entschlüsseln.

Give users key control for zero knowledge encryption

When users have control of the encryption key, they control access to the data, and can provide encrypted data to a password manager without the password management company having access to, or knowledge of, that data.

This is the fundamental premise on which well-designed password managers work. They facilitate strong and unique passwords that only you can access. Doing so requires zero knowledge of the secret data, and therefore users must control the encryption key. We refer to this as zero knowledge encryption.

But there is information beyond the secret Vault data that might be shared with a software or service provider. For example, an email address might serve as a unique customer identifier. One could claim that this isn't zero knowledge, and that would be correct.

At a minimum, zero knowledge must pertain to secret data. In the case of a password manager, that means all information within the password Vault. At the same time, it is important to recognize the realities of software, services, and users, and that in order for a commercial relationship to exist, their likely needs to be some knowledge exchanged between parties.

In the world of password managers, that line can get blurry. For example there are some password managers (not Bitwarden) that retain unencrypted URLs and websites for which you store passwords. While they claim that this benefits users, ultimately it provides these companies with detailed information on which websites users visit, when they do so, and every log in.

Bitwarden takes a more conservative view of what constitutes sensitive data, and therefore encrypts all of the information in your Vault, including the websites you visit, even the names of your individual items and folders. We use the term zero knowledge encryption because only you retain the keys to your Vault, and the entirety of your vault is encrypted. Bitwarden cannot see your passwords, your websites, or anything else that you put in your Vault. Bitwarden also does not know your Master Password. So take good care of it, because if it gets lost, the Bitwarden team cannot recover it for you.

Zero trust as a protective mindset

The zero trust model initially emerged as a way for organizations to get beyond the traditional thinking of internal and external threats to their IT operations. Today, companies need to protect from threats coming from both inside **and** outside. Zero Trust models often use technologies like identity and access management, encryption, multi-factor authentication, and permissions to operate.

Of course, between password managers and users adopting software or services, there is likely going to be at least **some** element of trust between the two parties. The password management provider trusts that the user will not violate the terms of service, and the user trusts that the password management provider will live up to their stated offering. However, everyone is better off if the boundaries of required trust are limited, so that even the possibility of sensitive data being compromised is eliminated altogether, hence the zero trust model.

While we stand by to support our customers with a trusted relationship, we can reduce the reliance on implied trust through the Bitwarden self-hosted offering. This deployment enables businesses with greater flexibility and control over their infrastructure. Running your own Bitwarden instance could be on an airgap network, further reducing risks by being disconnected from the internet.

At Bitwarden we take this trusted relationship with our users seriously. We also built our solution to be safe and secure with end-to-end encryption for all Vault data, including website URLs, so that your sensitive data is "zero trust" secure.

Understand and adopting safe encryption practices

We want our users to be well-informed on security practices in general, and with the benefits Bitwarden provides. With encryption, seek a complete end-to-end encryption architecture where only the end user retains the key, and make sure all sensitive data is encrypted using that architecture.

For many, it is easier to understand zero knowledge than end-to-end encryption, and we like easy! But we also understand the intricacies of these terms and aim to maintain clear definitions. We hope this article helps clarify our philosophy and approach.

Wenn Sie noch heute eine Zero Knowledge-Verschlüsselungslösung ausprobieren möchten, können Sie sich hier für ein kostenloses Bitwarden-Konto anmelden.