**Klant info beveiliging onderzoeks document**

Inhoud

[Introductie 3](#_Toc177548153)

[Literatuur onderzoek 4](#_Toc177548154)

[Methodologie 5](#_Toc177548155)

[Resultaat 6](#_Toc177548156)

[Conclusie 7](#_Toc177548157)

[Referenties 8](#_Toc177548158)

# Introductie

Wanneer een klant iets koopt van een web shop zal die adres info moeten invullen zodat het bestelde goed op de correcte locatie geleverd wordt. Om ervoor te zorgen dat de informatie van de klant niet door derde partijen met slechte bedoelingen gebruikt wordt zijn er verschillende beveiliging methodes beschikbaar tijdens het maken van de web shop. In dit document worden er enkele methodes besproken en geconcludeerd met welke methodes ik zal gebruiken in de opzet van mijn web shop.

# Literatuur onderzoek

Aangezien er veel verschillende manieren zijn van het beveiligen van gebruikers informatie zal ik in dit document 5 veel voorkomende beveiligingsmethodes bespreken. De vijf methodes die ik ga bespreken zijn Encryption, tokenization, data At Rest Encryption, PCI-DSS compliance en Multi-Factor Authentication.

## Encryption

Encryptie is een methode om de gegevens van een gebruiker te beschermen via TLS (Transport Layer Security). Dit werd vroeger gedaan via SSL (Secure Sockets Layer), maar TLS is een nieuwer en veiliger ontwikkelde versie van SSL. TLS beschermt gegevens die via het internet worden verzonden en voorkomt dat hackers en de dienstverlener de gegevens die tussen een klant (klant) en server (webshop) worden verzonden, kunnen bekijken of manipuleren. Deze vorm van beveiliging is verplicht geworden om de gevoelige informatie van gebruikers te beschermen (What Is SSL/TLS Encryption?, n.d.).

TLS is opgedeeld in twee delen: asymmetrische encryptie en symmetrische encryptie. Asymmetrische encryptie wordt eerst uitgevoerd en wordt gebruikt om een beveiligde verbinding tussen klant en server tot stand te brengen, terwijl symmetrische encryptie wordt gebruikt om gegevens uit te wisselen binnen de beveiligde sessie (What Is SSL/TLS Encryption?, n.d.).

Om TLS te gebruiken, moet een website een SSL-certificaat hebben (de naam is niet veranderd naar TSL-certificaat omdat de naam SSL-certificaat te veel wordt gebruikt, maar een SSL-certificaat biedt nog steeds TLS en geen SSL). Dit certificaat kost geld en gemiddeld ligt de prijs rond de $60 per jaar, maar kan oplopen tot $1000 per jaar, afhankelijk van het niveau van het certificaat (G, 2024).

## Tokenization

Tokenization wordt gebruikt in meerdere sectoren zoals AI, web3 (denk aan dingen zoals bitcoin en non-fungible tokens) en betalingen. AI en web3 zijn niet relevant voor dit onderzoek en worden daarom verder genegeerd. Door tokenization te gebruiken voor betalingen worden de gegevens die voor de betaling worden gebruikt verborgen, waardoor fraude wordt voorkomen (What Is Tokenization?, 2024).

Het gebruik van tokenization vereist een privé blockchain-ledger. Deze ledger toont welke transacties zijn uitgevoerd en wat deze hebben gekost (What Is Tokenization?, 2024). Echter, deze ledger toont alleen wat er gebeurt en bevat geen van de weergegeven waarden, dus als het geld van een account wordt gestolen, kan het verloren geld niet via de blockchain worden teruggedraaid. Een aparte database moet worden gebruikt om eventuele geleden schade te herstellen.

## Data At Rest Encyption

DARE (Data At Rest Encryption) verschilt van de eerder besproken encryptie, omdat het gericht is op het beschermen van gegevens die niet via een netwerk worden verplaatst. Dit type encryptie bestaat om een hiërarchie te creëren over wie wat mag inzien. Niet elke medewerker zou toegang moeten hebben tot de diepste delen van de webshop (Emptoris Strategic Supply Management 10.1.3, n.d.).

DARE wordt gebruikt op het niveau van databases. Omdat het niet interacteert met het internet, is het niet bruikbaar voor het beveiligen van klantinformatie wanneer gegevens van de klant naar de server en terug worden verzonden, maar het is perfect geschikt om ervoor te zorgen dat elk account en persoonlijke informatie van de klant goed beschermd is.

## PCI-DSS Compliance

PCI-DSS Compliance gaat over de minimale beveiliging waar een website aan moet doen zodra er persoonlijke gegevens van een klant gebruikt worden voor betalingen of soortgelijke gebeurtenissen. In het geval van betalingen moet een website de creditcard informatie van een klant zo goed mogelijk beveiligen zodat die niet publiekelijk te zien zijn. Veel bedrijven gebruiken derde partijen om aan PCI-DSS te voldoen (Stripe en PayPal zijn veelvoorkomende derde partijen hiervoor) (*Wat Is PCI DSS-compliance? 12 Vereisten | Stripe*, n.d.).

PCI-DSS heeft drie hoofdonderwerpen waar een website aan moet voldoen.

1. Het veilig overdragen van creditcard informatie van klanten.
2. Een veilige opslag plaats van persoonlijke gegevens.
3. Een jaarlijkse audit om te testen op veiligheid risico’s en veiligheid daarmee te valideren.

Aangezien PCI-DSS compliance meer een generieke methoden is die aangeeft waar een website minimaal aan moet voldoen wanneer het in contact komt met persoonlijke informatie van klanten heeft het geen tool/tools zoals andere methoden en eist het gebruik van sommige methoden (Wat Is PCI DSS-compliance? 12 Vereisten | Stripe, n.d.).

## Multi-Factor Authentication

Multi-Factor Authentication (MFA) verwijst naar het maken van twee of meerdere stappen om in te loggen op een website of andere service. Dit wordt gedaan om het hacken van accounts moeilijker te maken door meer informatie te vereisen voordat inloggen mogelijk is. denk aan het gebruik van een gebruikersnaam en wachtwoord en dan een pincode in moeten vullen. Deze extra laag beveiliging zorgt ervoor dat een account veilig blijft zelfs als een gebruikersnaam en wachtwoord gestolen worden (*Versterk Uw IT-beveiliging Met Multi-Factor Authenticatie (MFA)!*, 2024).

# Methodologie

Voor dit onderzoek ga ik de informatie van het literatuur onderzoek gebruiken als basis voor het creëren van een veilige web shop die de informatie van klanten veilig houdt.

# Resultaat

Uit dit onderzoek is het belangrijkste deel van een veilige web shop maken voldoen aan de eisen van PCI-DSS dit zal er wel om vragen om de andere methodes te gebruiken maar dit garandeert een veilige omgeving voor klanten.

# Conclusie

Voor mijn web shop zal ik PCI-DSS volgen om een veilige web shop te maken. Ik zal hiervoor encryption en data at rest encryption gebruiken om de persoonlijke informatie van mijn klanten veilig te houden.

# Referenties

*What is SSL/TLS Encryption?* (n.d.). F5, Inc. <https://www.f5.com/glossary/ssl-tls-encryption>

G, M. (2024, July 1). *SSL certificate cost in 2024: How much to spend on an SSL certificate*. Hostinger Tutorials. <https://www.hostinger.com/tutorials/ssl-certificate-cost>

*What is tokenization?* (2024, July 25). McKinsey & Company. <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-tokenization>

*Emptoris Strategic Supply Management 10.1.3*. (n.d.). <https://www.ibm.com/docs/en/strategicsm/10.1.3?topic=security-data-rest-encryption>

*Wat is PCI DSS-compliance? 12 vereisten | Stripe*. (n.d.). <https://stripe.com/nl/guides/pci-compliance>

*Versterk uw IT-beveiliging met Multi-Factor Authenticatie (MFA)!* (2024, June 20). Identity Management | Tools4ever. <https://www.tools4ever.nl/kennisbank/multi-factor-authenticatie-mfa/>