Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Assurance:

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Door: Gerard Bottemanne, GBNED

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Assurance:

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Wie kent dit rapport?

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Aanleiding

Als het gaat om het beoordelen van de beveiliging van (web)applicaties komen we standaarden tegen als: ISO27001, ISO27002, ISAE 3402, OWASP en SOC 2. Tel hierbij op termen als Injection, SQL-injectie en Cross-Site Scripting (XSS) en menig lezer haakt al snel af.

- Aanleiding om eerst voor mij zelf e.e.a. eens op een rij te zetten.
- Verzamelde kennis samen te vatten in rapport voor de markt.

Dat maakt me nog geen specialist op dit gebied!

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

ISO / IEC 27001

- Welke aanbieder is ISO 27001 gecertificeerd?

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

ISO / IEC 27001

- Welke aanbieder is ISO 27001 gecertificeerd?

- Is hiermee de veiligheid van (web)applicaties aangetoond en zo ja HOE?

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

ISO / IEC 27001

Specificatie voor “Information **Security** Management System” (ISMS).
Het is dus een standaard voor informatiebeveiliging.

Doel:
Voorzien in eisen voor het opstellen, implementeren, onderhouden en continu verbeteren van een ISMS. Via de ‘Deming Cycle’: plan, do, check, act (PDCA).

Het “continu verbeteren” betekent dat een auditor over de jaren heen verbeteringen in het ISMS moet constateren.

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

ISO / IEC 27001

Kenmerken:

- Geen open standaard;
- Veel gebruikte standaard met in verlengde de ISO / IEC 27001 certificering;
- Applicatie **niet** doorzagen;
- Overige ISO27K normen optioneel;
- Continu verbeteren ISMS via PDCA-cyclus;
- Vraag is of de veiligheid van de (web)applicatie zelf aangetoond is;
- Talloze organisaties werkzaam op dit vlak.
- Scope certificering kan deelaspect zijn.

Iemand aanvullingen?

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

ISO / IEC 27001

PinkWeb is ISO/IEC 27001:2013 gecertificeerd

Pink Web Applications B.V. is gecertificeerd volgens de ISO/IEC 27001:2013 norm voor informatiebeveiliging.

De certificering geeft aan dat PinkWeb alle processen op het gebied van informatiebeveiliging goed op orde heeft en het informatiebeveiligingssysteem beschikt over een solide en veilige structuur.

ISO 27001:2013 toetst het managementsysteem van informatiebeveiliging. Klanten en gebruikers

Scope van certificering

De scope waarop PinkWeb is gecertificeerd is als volgt:

Het ontwikkelen, verkopen en beheren van online accountancy software.

Bij PinkWeb valt het hele bedrijfsproces dus binnen deze scope: alle maatregelen uit het normenkader zijn van toepassing verklaard in de Statement of Applicability en geïmplementeerd in de organisatie.

Download hier onze Statement of applicability.

"Certificering voor informatiebeveiliging

Certificaat


bsi.

Certificaat

INFORMATIEBEVEILIGINGSMANAGEMENTSYSTEEM - ISO/IEC 27001:2013

Pink Web Applications B.V.
Grote Spui 39
3813 EZ Amersfoort
Nederland

ISC 119

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

ISO / IEC 27002 enz.

- Detaillering van ISO / IEC 27001;
- Praktische invulling (how to);
- Richtinggevend en geen certificeringsnorm;

Meer informatie over deze andere ISO 27000 standaards (meer dan **30!**) is te vinden op www.27000.org.

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

OWASP

Open Web Application Security Project (OWASP) is een wereldwijde non-profit organisatie, gericht op het verbeteren van de beveiliging van software.

- OpenSource en gratis beschikbaar;
- Potentie een certificeringsstandaard te worden;
- OWASP Top 10; bewustmaking.
- Toegepast bij richtlijnen Nederlands Cyber Security Centrum (NCSC).

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

OWASP Top 10 Most Critical Web Application Security Risks

1. Injection; zoals SQL-injectie: “1959YNiXH#' OR ‘1' = ‘1”;
   (zie ook Factsheet “Help! Mijn website is kwetsbaar voor SQL-injectie”, NCSC)

2. Broken Authentication; identiteit gebruikers ongewild verschaffen.

3. Sensitive Data Exposure; bijv. niet versleutelen gevoelige gegevens.
   (tegenwoordig alle websites HTTPS).

4. Cross-Site Scripting (XSS); via invoer kwaadaardige code injecteren.

5. Enz.

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

SANS

Het SANS Instituut en het Center For Internet Security hebben hun krachten gebundeld met de Amerikaanse overheid.

Lijst met best practices voor cyberbeveiliging van firewalls tot veilige ontwikkeling.

De complete lijst bestaat op dit moment uit 20 onderwerpen:

1. Inventory of Authorized and Unauthorized Devices;
2. Inventory of Authorized and Unauthorized Software;
3. Secure Configurations for Hardware and Software;
4. Continuous Vulnerability Assessment and Remediation;
5. Enz…

Dagelijks nieuws voor specialisten.

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

3402

- ISAE 3402; standaard van de IFAC (International Federation of Accountants).
- Richtlijn 3402; standaard van de NOREA.
- Standaard 3402; van de NBA.

Audit bij service organisaties van uitbestede financiële bedrijfsprocessen.
Is sprake van een getrouwe weergave systeem bij service organisatie?

Iemand aanvullingen?

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

3402

Vragen:

- Wie is bekend met 3402?
- Kan een SAAS leverancier beschouwd worden als service organisatie?
- Zijn er service organisaties in de zaal?
- Is de veiligheid van (web)applicaties een issue?

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

SOC

Service Organization Control (SOC) reports.
(door American Institute of Certified Public Accountants – AICPA)

Dilemma 3402: geen security aspecten afgedekt.

Oplossing: **SOC 2**, met expliciet aandacht voor:
1. Security;
2. Availability;
3. Proces integrity;
4. Confidentialty;
5. Privacy.

Aandachtspunt is AVG
(compliance met wet- en regelgeving)

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

SOC

- SOC 1; vergelijkbaar ISAE 3402
- SOC 2; aandacht voor security aspecten
- SOC 3; verkort assurance rapport
  + werkzaamheden gelijk aan SOC 2;
  + voor bredere verspreiding;
  + logo en certificaat voor breder publiek.

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Conclusies en aanbevelingen

Vaak geen onderliggende beoordelingen
Leveranciers melden behaalde certificeringen/beoordelingen op hun website.
Maar vaak GEEN onderliggende beoordelingen.

KEURMERK ZEKER-ONLINE Boekhouden

UBL READY

BDO

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Conclusies en aanbevelingen

Normen niet altijd gratis openbaar
ISO / IEC 27001 en ISO 27002 niet gratis openbaar beschikbaar.

Onze voorkeur:
- Nationaal Cyber Security Centrum (NCSC); ICT-Beveiligingsrichtlijnen.
- OWASP.

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Conclusies en aanbevelingen

Niet altijd sprake van certificering

De Norea meldt het volgende:
Het gebruik van een 3402-rapportage is in de richtlijn geregeld. Artikel 53e en A48 bepalen dat het rapport alleen mag worden gebruikt door gebruikende entiteiten en hun accountants.

Een samenvatting of uittreksel van een 3402-rapport, bijvoorbeeld in de vorm van een persbericht of conclusie, voldoet niet aan de rapportage eisen die daar op grond richtlijn 3402 aan worden gesteld.

Wel inmiddels COS 3.

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Conclusies en aanbevelingen

Scope certificering

Een (web)applicatie kan bijvoorbeeld:

- Wel beoordeeld op gebied van veiligheid en interne procedures leverancier;
- Niet op aanwezigheid functionaliteit;
- Niet op klanttevredenheid;
- Niet op gebruikersgemak.

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Conclusies en aanbevelingen

Persoonlijke boodschap:
"*Laat je niet verleiden door alleen het melden van een logo als het gaat om certificering van een aanbieder en haar (web)applicaties. Zorg dat je inzicht krijgt in het volledige normenkader en, nog belangrijker, een rapport met een specificatie van de beoordeling. Zodat je kunt zien welke eigenschappen en aspecten wel of niet zijn beoordeeld en met welk resultaat.*

Beoordelen veiligheid (web)applicaties (en IT-organisaties)

Bron:
Gratis rapport *“Beoordelen veiligheid (web)applicaties (en IT-organisaties)”*

Vragen?