Guide til optimering af sikkerhed på Magento-webshops

Guiden er udarbejdet af TRIC Solutions
– Magento udviklinghus og sparringspartner.

TRIC Solutions
MAGENTO E-COMMERCE AGENCY

www.tric.dk

Sikring af shoppens data

- ❑ **Tag løbende backup af database og filer**
  Forhåbentligt har I allerede styr på denne del. Sørg for at der altid er en nylig backup tilgængelig, og at jeres gendannelsesprocedure er testet, således I kan stole på at det vil hjælpe jer hvis uheldet er ude. Det er typisk jeres hostingpartner, der håndterer disse backups.

Sikring mod udefrakommende angreb

- ❑ **Opdatér til seneste version og installér patches**
  Sørg for at shoppen altid er opdateret til seneste Magento-version, og at alle patches er implementeret.

- ❑ **Opdatér uddateret software på serveren**
  Sørg for at serveren ikke har installeret uddateret software, som har sikkerhedshuller og ikke vedligeholdes, som f.eks. PHP 5.5.

- ❑ **Brug sikret SFTP-forbindelse til serveren**
  Sørg for at hackere ikke kan gætte eller opfange FTP-adgangskoder.

- ❑ **Brug krypteret SSL/HTTPS-forbindelse**
  Sørg for at siden har et aktivt SSL-certifikat, der forhindrer hackere i at opsnappe informationer der sendes mellem browseren og serveren.

- ❑ **Konfigurér indbyggede sikkerhedstiltag**
  Der findes en række indbyggede indstillinger i Magento, som kan optimere sikkerheden i shoppen. Du bør kun ændre disse indstillinger, hvis du ved hvilken effekt de har på din shop, og ved at din shop/dit tema vil fungere med disse indstillinger. Fra administrationen tilgår du System -> Konfiguration -> Admin, og sætter følgende indstillinger.
  - ❑ Login er case sensitive -> Ja
  - ❑ Allow Magento Backend to run in frame -> Only from same domain
  - ❑ Enable Form Key Validation On Checkout -> Ja
  - ❑ Allow Magento Frontend to run in frame -> Only from same domain

- ❑ **Scan siden for kendte bugs i en række moduler**
  Magereport.com er et solidt værktøj, og ellers er Magento's eget tool er også godt: https://account.magento.com/scanner.

- ❑ **Fjern gamle og overflødige moduler**
  Moduler der ikke længere bruges eller vedligeholdes udgør en sikkerhedsrisiko og øger blot ens angrebs-vektor. Det gælder også for ens gamle Wordpress blog man ikke længere bruger.

- ❑ **Fjern mulighed for directory browsing (fx via htaccess)**

- ❑ **Sørg for at shoppen har de rigtige skrive- og læserettigheder til filer og mapper**

- ❑ **Begræns adgang til udvikling og staging-miljøer med .htaccess password**

Sikring mod utilsigtede forsøg på brugeradgang

- ❑ **Flyt administrationen til anden URL end standard**
  Sørg for at man ikke kan tilgå siden URL via /admin, som er standard for Magento.

- ❑ **Fjern andre veje til administrationen**
  Sørg for at man ikke kan logge ind på administration fra følgende URLs:
  /rss/catalog (overvej at deaktivere RSS, såfremt det ikke bruges)
  /downloader (overvej at deaktivere Magento Connect Manager, såfremt det ikke bruges)

- ❑ **Opsæt IP-begrænset adgang til administrationen**
  Blokér al adgang til sidens administration, som ikke kommer fra specifikke IP-adresser. Er dette for besværligt for at kunne administrere siden, kunne man overveje at lave en mulighed for let at tilføje disse IP'er udefra. Alternativt kunne man sørge for at administrationen kun må tilgås fra én specifik IP-adresse, som man så tilgår gennem en VPN-adgang.

- ❑ **Opsæt Two-Factor Authentication til administrationen**
  Log ind med to-trins-godkendelse via Google Authenticator eller Duo Security. Der findes flere moduler på markedet, der kan løse dette.

- ❑ **Opsæt Captcha-funktionalitet på loginside**
  Magento har en standard Captcha-funktionalitet, og ellers kan det anbefales at bruge Googles Recaptcha. Der findes også flere moduler derude, der kan løse dette.

- ❑ **Blokér forsøg på login med ikke-eksisterende brugernavne**
  Opsæt blokering af IP-adressen, såfremt der forsøges at logge ind med et brugernavn der ikke findes.

- ❑ **Undlad brug af brugernavnet "admin"**
  Sørg for at der ikke findes en bruger på shoppen med brugernavnet "admin".

Sikring mod kompromitteret brugeradgang

- ❏ **Kontrollér brugere og rettigheder**
  Hold styr på hvilke brugere der har adgang til shoppen, og hvilke rettigheder de har:
  - ❏ Fjern gamle brugere, der ikke bør have adgang længere
  - ❏ Sørg for at alle brugere er unikke pr. person, og ikke deles
  - ❏ Sørg for at alle brugere kun har rettigheder til de områder af shoppen som er nødvendig for deres arbejdsområde
  - ❏ Sørg for at brugere ikke har adgang til at rette deres egne rettigheder

- ❏ **Brug stærke passwords**
  Sørg for at alle brugerkonti har stærke passwords (læs: lange og gerne med en blanding af tegn, numre og symboler). Her kan man med fordel anvende Password-managers til at hjælpe med at huske adgangskoden.

- ❏ **Skift passwords jævnligt**
  Gør det besværligt at opfange eller gætte kodeord, ved at udskifte disse med jævne mellemrum.

- ❏ **Brug anti-virus på din computer**
  Bliver din computer inficeret med virus, kan det betyde at bagmanden kan opsnappe dine adgangskoder til forskellige sider, herunder login til din Magento.