STITCH 1.0

Het is steeds belangrijker dat software en diensten aan veiligheidseisen voldoen. Maar hiervoor zijn veel verschillende lijsten en leidraden; welke kies je dan? SCIRT, de community voor cybersecurity, heeft daarom een vereenvoudigde checklist ontwikkeld: De Security Technical IT CHecklist (STITCH).

Het principe van STITCH is eenvoudig: er is een baseline met een beperkt aantal eisen, deze eisen zijn eenvoudig te meten. Door deze uitgangspunten kunnen security officers veel sneller en eenvoudiger vaststellen of een dienst of software 'veilig' is.

De 8 STITCH punten:

- STITCH-1: Alle gegevens worden versleuteld getransporteerd
- STITCH-2: De identiteit van gebruikers is gecontroleerd en federatief beheerd
- STITCH-3: Autorisatie vindt plaats op basis van functiescheiding en least privilege
- STITCH-4: Veilig sessiemanagement wordt toegepast
- STITCH-5: Alle in- en uitvoer van data wordt genormaliseerd, gevalideerd en ingeperkt
- STITCH-6: Configuratie-lekken worden voorkomen
- STITCH-7: Systemen bieden voldoende mogelijkheden voor auditing en logging
- STITCH-8: Er vindt continu onderhoud en patchmanagement plaats

Uitwerking

STITCH 1) Alle gegevens worden versleuteld getransporteerd

De vertrouwelijkheid, integriteit en onweerlegbaarheid van gegevensleveringen of transacties dient geborgd te worden.

Risico's:

Ongeautoriseerde toegang tot diensten en inzien of muteren van gegevens.

Implicaties:

- Datatransport wordt volgens up-to-date encryptie-standaarden en standaard transportprotocollen versleuteld.
- Als het transportprotocol geen versleutelingsmogelijkheden biedt, moet de data versleuteld worden.
- Bij fysiek transport van gevoelige data, zoals USB-sticks, dient de data volgens up-to-date encryptie-standaarden versleuteld te zijn.
- Certificaatbeheer moet ingericht zijn.

Testen:

SSL Labs server test (https://www.ssllabs.com/ssltest/) met als testresultaat minimaal een A. Voor niet-publieke systemen is er ook een lokale scantool te downloaden bij SSL Labs.

Breng alle datastromen in kaart en controleer dat deze met up-to-date encryptie-standaarden versleuteld zijn.

Controleer bij IMAP, POP3, NNTP en LDAP of het STARTTLS commando wordt verstuurd nadat initieel een onveilige verbinding is opgezet. Zie voor nadere informatie: https://en.wikipedia.org/wiki/Opportunistic_TLS

Controleer dat Forward Secrecy wordt gebruikt, zodat communicatie ook vertrouwelijk blijft indien de sleutelbestanden in de toekomst uitlekken. Dit is ook te controleren door de SSL Labs server test.

Referenties:

- SSD: 4
- OWASP: https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet#Basic_Requirements
- ISO 27002:2013 13.1.1 13.2.1 14.1.2

STITCH 2) De identiteit van gebruikers is gecontroleerd en federatief beheerd

Instellingen dienen de identiteit van de gebruiker te controleren en applicaties werken met een persoonlijke identiteit. Dit zorgt ervoor dat handelingen terug te voeren zijn naar personen.

Risico's:

Misbruik van identiteit of niet herleidbaar misbruik van systemen. De gevolgen kunnen ongeautoriseerde onthulling van informatie, ongeautoriseerde modificatie of onterechte invoer van transacties uit naam van valide gebruikers zijn.

Implicaties:

- Webapplicaties maken gebruik van de identity provider van de instelling of SURFconext voor identificatie en authenticatie.
- Authenticatie gebeurt federatief zodat wachtwoorden niet buiten de eigen instellingsgrenzen beschikbaar zijn.
- Een lock-out mechanisme is ingesteld tegen brute-forcing.

Testen:

Controleer dat geen default accounts met default passwords aanwezig zijn en dat geen default SNMP community strings in gebruik zijn.

Test dat een gebruiker die geen autorisatie meer heeft in het centrale IDM-systeem ook geen toegang meer heeft tot de applicatie.

Controleer dat bij invoer van wachtwoorden na een beperkt aantal foute pogingen de toegang geblokkeerd wordt.

Referenties:

- SSD: 6
- ISO 27002:2013 18.1.1 9.2.4 9.2.1 9.2.6 9.4.2

STITCH 3) Autorisatie vindt plaats op basis van functiescheiding en least privilege

Applicaties dienen gebruik te maken van functiescheiding. Op basis van taken, verantwoordelijkheden en bevoegdheden zijn in de applicatie rollen gedefinieerd. Hierbij is extra aandacht voor accounts met hoge privileges.

Risico's:

Het ontbreken van functiescheiding kan leiden tot fraude of misbruik van bedrijfsmiddelen bij kritische of fraudegevoelige taken.

Indien een gebruiker over te hoge rechten beschikt kan daar misbruik van worden gemaakt en bestaat het risico dat bij het compromitteren van een account onnodige schade ontstaat.

Implicaties:

De applicatie beschikt over ingericht rollenbeheer.

Testen:

Controleer of een nieuw gemaakt account geen of alleen basis rechten heeft. Voeg rollen toe en controleer of de verkregen rechten overeenkomen met de rechten die bij de betreffende rollen horen.

Referenties:

- SSD: 7,8
- ISO 27002:2013: 6.1.2 9.1.2 9.2.2 9.4.1

STITCH 4) Veilig sessiemanagement wordt toegepast

Misbruik van bestaande sessies dient te worden tegengegaan door sessiemanagement in te richten.

Dan kan middels het toevoegen van security headers bij gebruik van HTTP. Andere protocollen zoals SMTP, IMAP, POP3 en SSH moeten op andere manieren worden beveiligd.

Risico's:

Misbruik van bestaande sessies, zoals overname van sessies en man-in-the-middle-aanvallen.

Implicaties:

- Gebruik HTTP-headers, zie https://securityheaders.com
- Richt sessiemanagement in, zie: https://www.owasp.org/index.php/Session_Management_Cheat_Sheet
- Gebruik sessie-cookies met 'HttpOnly' en 'Secure' flags.

Testen:

Maak voor het testen gebruik van de OWASP Session Management Cheat Sheet en de bijbehorende testmethodiek. Dit document legt uit hoe sessiemanagement goed in te richten is. Let vooral op zaken als veilig transport en verlooptijd van de sessie. Zie: https://www.owasp.org/index.php/Testing_for_Session_Management_Schema_(OTG-SESS-001)

Controleer de HTTP security-headers met de online scan van https://securityheaders.com/.

Stel vast dat de flags ‘HttpOnly’ en 'secure' op sessie-cookies zijn ingesteld.

Controleer sessie-termination.

Referenties:

- SSD: 12
- ISO 27002:2013: 11.2.8 9.4.2
- W3C: https://www.w3.org/TR/CSP3/

STITCH 5) Alle in- en uitvoer van data wordt genormaliseerd, gevalideerd en ingeperkt

Data-integriteit dient te worden gewaarborgd. Veel aanvallen zijn op basis van invoer van verkeerde data in applicaties.

Risico's:

Het achterwege laten van normalisatie, validatie en inperking van in- en uitvoer verhoogt de kans op uitbuiting van kwetsbaarheden. Dit kan leiden tot inbreuk op data-integriteit en op vertrouwelijkheid van data.

Verspreiding van malware via in- en uitvoer van besmette bestanden.

Implicaties:

Bij in- en uitvoer van data moet normalisatie, validatie en inperking toegepast worden.

Documenten moeten indien nodig worden omgezet in een formaat dat geen schade kan aanrichten.

Testen:

Controleer met vulnerability scanners op kwetsbaarheden zoals SQL injection en XSS. Ter ondersteuning kunnen bestaande recente testrapporten worden opgevraagd of een pentest uitgevoerd worden.

Voorbeelden van kwetsbaarheden zijn:

- Invoervelden waar injectieaanvallen mogelijk zijn.
- File includes van bestanden op remote sites die door derden kunnen worden gemanipuleerd.
- Bestanden zoals documenten waarin schadelijke macro's aanwezig kunnen zijn.
- Webservers die directory listings tonen.

Referenties:

- SSD: 18, 19, 20, 21, 22, 23, 29
- OWASP: https://www.owasp.org/index.php/Data_Validation
- ISO 27002:2013 14.2.1

STITCH 6) Configuratie-lekken worden voorkomen

Het lekken van configuratiegegevens in headers, banners en error pagina's dient voorkomen te worden.

Risico's:

Dit kan gebruikt worden om informatie over de server en softwareversies te bemachtigen en overige configuratie van de applicatie te achterhalen.

Implicaties:

- Banners en headers dienen geen configuratiegegevens te lekken.
- Foutpagina's dienen geen configuratiegegevens te lekken. Denk hierbij aan stacktraces en interne debug-informatie.
- Commentaar in code wordt niet aan eindgebruikers getoond.

Testen:

- Scan met een vulnerability scanner voor banner grabbing en fingerprinting.
- Controleer fout pagina's op inhoud.
- Zoek naar onbedoeld publiek toegankelijke databasedumps en backups.
- Controleer client-side code op commentaar.
- Stel handmatig of met behulp van tools zoals URL fuzzers vast, dat bestanden niet rechtstreeks zijn te benaderen.

Referenties:

- SSD: 2, 24, 25, 26, 27
- RFC7762, RFC7508

STITCH 7) Systemen bieden voldoende mogelijkheden voor auditing en logging

Systemen dienen auditing en logging ingericht te hebben.

Logging in systemen is nodig om beheerwerkzaamheden en storingen te kunnen monitoren. Dit omvat ook het loggen van foutmeldingen.

Auditbaarheid, via audit logging, van systemen is nodig om de integriteit en vertrouwelijkheid van data te kunnen waarborgen. Verder is dit nodig om te kunnen herleiden wat er in de applicatie is gebeurd en door wie en wanneer dit is gedaan.

Risico's:

Voor logging: Tekortkomingen en zwakheden in de applicatie kunnen niet gesignaleerd worden en herstelacties kunnen bij gebrek hieraan niet tijdig worden genomen.

Voor auditing: Beveiligingsincidenten kunnen niet afgehandeld worden en er ontbreekt bewijsmateriaal.

Implicaties:

- Logging en auditing worden opgeslagen.
- Logging en auditing is beveiligd tegen ongeautoriseerde toegang.
- Logging en auditing is voldoende gedetailleerd zodat incidenten herleid kunnen worden naar natuurlijke personen.

Testen:

Controleer logging en auditing op de volgende punten:

- Er is voldoende informatie aanwezig voor beheerwerkzaamheden en storingsdetectie.
- Auditing is tot een persoon te herleiden.
- Logging wordt weggeschreven naar een logbestand of een centrale logserver.

Referenties:

- SSD: 9, 13, 27, 30
- ISO 27002:2013: 12.4.1.12.4.3

STITCH 8) Er vindt continu onderhoud en patchmanagement plaats

Er kunnen kwetsbaarheden in applicaties worden ontdekt. Om veilig te kunnen werken dienen applicaties continu onderhouden te worden en patches te worden ontwikkeld en uitgevoerd.

Risico's:

Als de applicatie niet meer actief wordt onderhouden, worden er geen patches meer ontwikkeld. Applicaties die achterlopen met patches kunnen kwetsbaarheden bevatten.

Implicaties:

- Patchmanagement moet ingericht worden.
- Nieuwe relevante CVE's dienen tijdig door ontwikkelaars te worden geadresseerd.
- End-of-life applicaties worden niet gebruikt.

Testen:

- Controleer dat de applicatie nog doorontwikkeld wordt, aan de hand van onder andere recente patches, documentatie en een actieve community.
- Stel vast dat recent patches zijn uitgebracht en toegepast bijvoorbeeld met een vulnerability scanner.

Referenties:

- ISO 27002:2013: 12.5.1 12.6.1 14.2.2
- SSD 1

Bronvermelding

- ISO: International Organization for Standardization - https://www.iso.org
- SSD: Grip op Secure Software Development - https://www.cip-overheid.nl/wp-content/uploads/2018/01/Grip-op-SSD-Beveiligingseisen-v2_0.pdf
- OWASP: Open Web Application Security Project - https://www.owasp.org
- RFC: Request For Comments - https://www.ietf.org/standards/rfcs/
- W3C: World Wide Web Consortium (W3C) - https://www.w3.org
- SSL Labs: SSL Labs server scan: - https://www.ssllabs.com
- Securityheaders.io: Securityheaders scan - https://www.securityheaders.io

Randvoorwaarden

Voor de STITCH eisen gelden een aantal randvoorwaarden waaraan hoe dan ook voldaan dient te worden. Dit kunnen bijvoorbeeld wettelijke en organisatorische randvoorwaarden zijn op het gebied van informatiebeveiliging en privacybescherming.

Wettelijke randvoorwaarden:

- Aan de AVG wordt voldaan.
- Standaarden op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie die van toepassing zijn op de organisatie.

Organisatorische randvoorwaarden:

- De architectuurprincipes van de organisatie worden gevolgd.
- Alle data wordt geclassificeerd volgens de geldende classificatierichtlijnen.
- Het informatiebeveiligheidsbeleid van de organisatie wordt gevolgd.
- Shadow-IT, eilandautomatisering en ad-hoc oplossingen worden vermeden. Er wordt gebruikgemaakt van standaard bouwblokken voor zover deze in de organisatie aanwezig zijn.
- Naamgevingsconventies t.a.v. DNS en servernamen worden gevolgd.