SECURITY ASSESSMENT RAPPORT

VOOR

DIGITALE POLI

PROJECT	ASSESSMENT EXTERNE IT-OMGEVING
SERVICETYPE	INFRA/APPLICATION TEST
DOCUMENTREFERENTIE	SLA_DIGP_0314-1
DOCUMENTEIGENAAR	DIGITALE POLI
AUTEUR	ILIAS EL MATANI
DATUM	DONDERDAG 12 JUNI 2014
TESTPERIODE	19-05 T/M 22-05-2014

THIS REPORT MAY CONTAIN CONFIDENTIAL COMPANY INFORMATION.
ACCESS SHOULD BE RESTRICTED TO AUTHORIZED PERSONNEL.

Managementsamenvatting

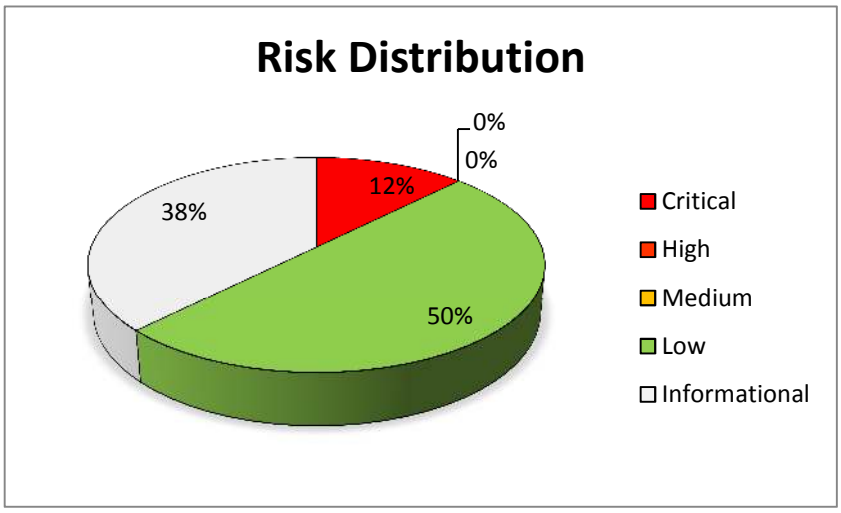
Inleiding

SecureLabs is verheugd door Digitale Poli te zijn gekozen voor het uitvoeren van de aanval- en penetratietest.

SecureLabs beschikt over Senior Information Security Consultants en Security engineers. Zij zijn consultants en professionals met uitgebreide kennis en ervaring op het gebied van Enterprise Security en gecertificeerd bij het International Information Systems Security Certification Consortium (ISC^2) met de titel en erkenning van Certified International Information Systems Security Professionals (CISSP).

Samenvatting dreigingen

Het assessment resulteerde in acht bevindingen waarvan één was geclassificeerd als een critical. Deze kwetsbaarheid is direct opgepakt en na de hertest is deze kwetsbaarheid niet meer geconstateerd. Zie onderstaande afbeelding en tabel voor een overzicht van de risico's.



Risk	Number
Critical	1
High	0
Medium	0
Low	4
Informational	3
Total	7

Conclusie

SecureLabs heeft in opdracht van Digitale Poli haar gelijknamige webapplicatie getest. Tijdens deze test zijn er twee bevindingen aangetroffen binnen de Digitale Poli applicatie.

De eerste bevinding was een stored cross site scripting waarbij een gebruiker een bepaalde string kon opslaan waarna alle andere gebruikers van de Digitale Poli applicatie door deze cross site scripting fout geraakt konden worden. De fout had in potentie het risico om sessie van gebruikers te stelen. Digitale Poli heeft deze fout nog tijdens de testen van SecureLabs opgelost en SecureLabs heeft deze oplossing tijdens de test ook meteen gecontroleerd en geconstateerd dat de kwetsbaarheid niet meer aanwezig was in de applicatie.

De tweede kwetsbaarheid die is aangetroffen zit in het vergrendelscherm. De Digitale Poli webapplicatie heeft een functionaliteit waarbij het scherm van de browser zich 'locked' wanneer een gebruiker een bepaalde tijd inactief is. Dit is een betere oplossing dan waarbij een scherm ge-unlocked blijft en waarbij alle gegevens open blijven staan op het scherm.
Doordat het lock scherm actief wordt krijgen gebruikers de impressie dat niemand bij de gegevens die de gebruiker open heeft kan komen. Echter het lock scherm wordt bovenop de webpagina binnen de browser gelegd. De browser en de computer van de gebruiker blijven gewoon benaderbaar en hierdoor kan iemand de broncode kan opvragen. In deze broncode die op de browser aanwezig kan iemand nog de gegevens halen die de gebruiker op zijn/haar scherm had staan.
Onlangs deze kwetsbaarheid is het lock scherm wel een pre tegenover het open laten staan van het scherm, dit omdat wanneer het scherm zonder lock open zou blijven staan iemand doormiddel van shoulder surfing de gegevens die op het scherm aanwezig zijn kan inzien. Er hoeft geen contact gemaakt te worden met de computer van de gebruiker. Door de lock is het zelfde nog wel mogelijk alleen moet iemand plaatsnemen achter de computer en moet handelingen uitvoeren om het zelfde resultaat te verkrijgen.

Voor de rest heeft SecureLabs geen bevindingen aangetroffen in de applicatie. Wel in de infrastructuur maar ook deze issues zijn op het moment van het maken van de rapportage al opgelost.

Het algemene beeld van de Digitale Poli applicatie is goed, de ontwikkelaars zijn zeer security minded bezig, issues die worden aangetroffen worden zeer snel opgepakt en ook zijn best practices zoals bijvoorbeeld HSTS dat er voor zorg dat browsers ook geforceerd via de middels SSL beveiligde verbinding lopen zijn al op het moment van testen geïmplementeerd. Iets wat SecureLabs tijdens de werkzaamheden bij vele klanten in diverse sectoren niet veel ziet.

Aanbevelingen

Het is belangrijk bij iedere nieuwe release of aanpassing van de applicatie of infrastructuur de beveiliging te controleren. Fouten worden snel gemaakt onlangs de awareness en mindset van beheerders en ontwikkelaars.
Een penetratietest is slechts een momentopname waardoor het raadzaam is om penetratietesten periodiek uit te laten voeren.