

Consultancy

Volwassen(er) informatiebeveiliging, van techniek tot beleid, door een bottom-up en top-down verandering, op basis van security expertise, psychology en agile methodieken

Solutions

Volledige oplossingen in samenwerking met derden of gebouwd op maat, van oriëntatie tot uitsluiting; inclusief integratie, implementatie en training; professioneel, doelmatig, betaalbaar

Research

Kwetsbaarheid-analyse, penetratietest / intrusion test (systeem, netwerk, web, mobile), technical audit, forensisch onderzoek, social engineering onderzoek; oplossingsgericht, doelmatig advies

Waarom onze diensten

- inschatten risico's, dreigingen, kwetsbaarheden
- inzicht vergaren in stand van beveiliging
- richting en prioriteit geven aan verbeteringen
- voldoen aan wet- en regelgeving, policies
- realiseren van (iteratief) beveiligingsproces
- voorkomen van incidenten, minimaliseren van gevolgen
- optimaliseren van informatiebeveiliging
- beschermen

Waarom Le Reseau

- wij geloven dat succesvolle informatiebeveiliging een proces is waarmee de organisatie in staat is zichzelf voortdurend beter te beschermen. wij ondersteunen onze klanten in de realisatie en optimalisatie van dit proces.
- In elke dienst of oplossing die wij leveren staan wij voor maximale professionaliteit en kwaliteit, die haar waarde behoudt lang na afronding van onze dienstverlening.

Solutions

- anti exploit (Le Reseau Protector)
- software van derden
- realisatie maatwerk

Research

- security assessment
- penetratie-/‘intrusion’ test
- social engineering test
- analyse & advies
- proces & beleid
- digitale forensics

Consultancy

- implementatie agile security processen
- integratie menselijke factoren
- top-down / bottom-up change management

Voorkennis / rechten

- black box: geen / zeer beperkt
- grey box: beperkt, opdrachtgever bepaalt
- white box: veel / alles, onderzoeker bepaalt

Onderwerpen

- applicatie
- website
- systeem
- netwerk
- beleid
- mens
- informatie
- juridisch
- media
- proces

Werkwijze

- vraagstelling
- afspraken
- plan en planning
- uitvoering
- rapportage
- toelichting
- perspectief

Resultaat (rapport)

- bevindingen
- toelichtingen
- verbeteradviezen
- externe referenties
- normverwijzing
- CVSS scores
- algemeen advies
- samenvatting

Resultaat

- realisatie / optimalisatie (agile) informatiebeveiligingsproces
- implementatie en integratie wereldwijde standaarden en best-practices
- top-down & bottom-up change
- risico minimalisatie

Integratie Aanbod

Consultancy

Volwassen(er) informatiebeveiliging, van techniek tot beleid, door een bottom-up en top-down verandering, op basis van security expertise, psychology en agile methodieken

Solutions

Volledige oplossingen in samenwerking met derden of gebouwd op maat, van oriëntatie tot uitsluiting; inclusief integratie, implementatie en training; professioneel, doelmatig, betaalbaar

Research

Kwetsbaarheid-analyse, penetratietest / intrusion test (systeem, netwerk, web, mobile), technical audit, forensisch onderzoek, social engineering onderzoek; oplossingsgericht, doelmatig advies

Pakketten

- Scan
- Assessment
- Improvement
- Maturity

Security Scan

- 'best-effort' onderzoek; afhankelijk van beschikbare tijd & voorkennis
- gestandaardiseerde testuitvoering
- uitvoering primair door geautomatiseerde processen
- levert indicaties van kwetsbaarheden, engelstalig (optioneel nederlands)
- CVSS risico scores zonder omgevingsfactoren
- algemene adviezen, 'fix' van kwetsbaarheid
- beknopte managementsamenvatting

Security Assessment

- 'best-effort' onderzoek; afhankelijk van beschikbare tijd & voorkennis, op basis van standaarden en situatie opdrachtgever
- gestandaardiseerde testuitvoering
- gecombineerd handmatig en geautomatiseerd onderzoek
- standaardisatie volgens wereldwijd erkende standaarden van kwetsbaarheden en achterliggende problematiek
- realistische risico inschatting, inclusief omgevingsvariabelen, genormeerd volgens de gestandaardiseerde CVSS scoring
- advies in context van de situatie van de opdrachtgever, gericht op het voorkomen en herstel van problemen
- managementsamenvatting met visuele weergaven en situatie overzicht

Security Improvement

- daadwerkelijke verbetering van beveiliging van informatie en processen door op een agile wijze, doelmatig Consultancy en Research te combineren, tegen minimale belasting en kosten
- preventie en structurele verbetering door een gecombineerde aanpak van bottom-up / top-down interventie
- professionalisering van projecten en werkprocessen door (geleidelijke) implementatie van gestandaardiseerde 'security-eisen' en normen, conform wereldwijde standaarden (e.g. OWASP, PCI, COBIT, ISO 27xxx)
- beheersing en controle door betere implementatie van monitoring en doelmatige documentatie-eisen
- blijvende en zelflerende verbetering door kleinschalige, realiseerbare veranderingen, zelf-educatie, bottom-up en top-down integratie en communicatie

Integratie Aanbod

Consultancy

Volwassen(er) informatiebeveiliging, van techniek tot beleid, door een bottom-up en top-down verandering, op basis van security expertise, psychology en agile methodieken

Solutions

Volledige oplossingen in samenwerking met derden of gebouwd op maat, van oriëntatie tot uitsluiting; inclusief integratie, implementatie en training; professioneel, doelmatig, betaalbaar

Research

Kwetsbaarheid-analyse, penetratietest / intrusion test (systeem, netwerk, web, mobile), technical audit, forensisch onderzoek, social engineering onderzoek; oplossingsgericht, doelmatig advies

Pakketten (vervolg)

- Scan
- Assessment
- Improvement
- Maturity

Security Maturity

- een volwassen(er) informatiebeveiliging gericht op voortdurende groei, op basis van bredere implementatie van het Security Improvement model, waarbij het model ook onderdeel is van het groeiproces.
- bottom-up en top-down benadering van procesverandering, verbetering informatiebeveiliging conform wereldwijd erkende standaarden, normen en procedures (e.g. ISO 27xxx, COBIT, PCI, OWASP)
- een volledige oplossing, multi-disciplinair, gebaseerd op parallelle agile processen, waarbij gelijktijdige, kleinschalige, haalbare verbeteringen worden gerealiseerd op meerdere niveaus binnen de organisatie
- continuïteit van groei door educatie, bewustwording, training en overdracht van kennis en expertise, zodat de organisatie zelf kan voortbouwen op de dienstverlening van Le Reseau

Achtergrond - Research

Consultancy

Volwassen(er) informatiebeveiliging, van techniek tot beleid, door een bottom-up en top-down verandering, op basis van security expertise, psychology en agile methodieken

Solutions

Volledige oplossingen in samenwerking met derden of gebouwd op maat, van oriëntatie tot uifasering; inclusief integratie, implementatie en training; professioneel, doelmatig, betaalbaar

Research

Kwetsbaarheid-analyse, penetratietest / intrusion test (systeem, netwerk, web, mobile), technical audit, forensisch onderzoek, social engineering onderzoek; oplossingsgericht, doelmatig advies

Research

- 'fix' of oplossing?
- standaarden
- agile

'fix' of oplossing

- security testen is bedoeld om risico's in te schatten, door kwetsbaarheden te vinden binnen een informatieomgeving
- door de complexiteit en oneindigheid van mogelijkheden kan een security test per definitie niet alle kwetsbaarheden vinden.
- een kwetsbaarheid impliceert veelal een structureel probleem, dat zelden tot nooit wordt geadresseerd in conventionele security testen.
- Le Reseau probeert door middel van standaarden, expertise en ervaring de achterliggende oorzaak van een kwetsbaarheid vast te stellen en een daadwerkelijke oplossing te adviseren, niet uitsluitend een 'fix' of tijdelijke work-around.

standaarden

ondanks het 'best-effort' karakter van security testen zijn er op diverse niveaus standaarden, normenkaders, baselines en 'guides'. Voor kwaliteit, uniformiteit en algemene professionaliteit maakt Le Reseau gebruik van deze standaarden waar mogelijk.

- standaardisatie testuitvoering, ter 'guide'.
 - e.g. web security onderzoek: OWASP Test Guide Checklist
- standaardisatie benoeming kwetsbaarheden, optioneel
 - e.g. web kwetsbaarheden: OWASP Top 10
 - e.g. software kwetsbaarheden: CSV-database
- standaardisatie inschatting risico scores
 - CVSS v2 risico inschatting, inclusief temporal en environmental scores
- standaardisatie eisen ter voorkoming van de achterliggende problemen
 - e.g. web security eisen (requirements): OWASP ASVS
- realisatie van conformering aan normen
 - e.g. ISO 27001/2

agile

- security is een voortdurend verbeterproces. Le Reseau ondersteunt voortdurende verbetering, waarbij het zelflerende karakter cruciaal is.
- proces: test > kwetsbaarheid > achterliggend probleem > structurele oplossing / eventueel fix > gestandaardiseerde requirements toekomst + policy update > test...

Achtergrond - Organisatie

Consultancy

Volwassen(er) informatiebeveiliging, van techniek tot beleid, door een bottom-up en top-down verandering, op basis van security expertise, psychology en agile methodieken

Solutions

Volledige oplossingen in samenwerking met derden of gebouwd op maat, van oriëntatie tot uitsluiting; inclusief integratie, implementatie en training; professioneel, doelmatig, betaalbaar

Research

Kwetsbaarheid-analyse, penetratietest / intrusion test (systeem, netwerk, web, mobile), technical audit, forensisch onderzoek, social engineering onderzoek; oplossingsgericht, doelmatig advies

Le Reseau

- organisatie
- partners
- backup

organisatie

- sinds 1992, in diverse vormen, security advisering en testen
- sinds 2006, onder leiding van D. Dubbelhuis
- nieuwe organisatievorm: minimaal personeelsbestand, maximale samenwerking op basis van freelance experts en deskundigen (altijd na verklaring omtrent gedrag / screening), ter garantie maximale expertise
- opdrachtgevers omvatten overheidsorganen, suboverheden, zorginstellingen, educatieve instellingen en universiteiten, software leveranciers en -ontwikkelaars, uitgevers, verzekeraars, internationale commerciële organisaties, juridische dienstverleners, MKB(+), not-for-profit organisaties en incidenteel privé-personen
- kwaliteit, professionaliteit, innovatie zijn de kernfactoren

partners

- om een breed scala aan diensten te kunnen bieden werken we samen met
 - auditors / accountants
 - IT juristen
 - onafhankelijke security experts
 - compliancy experts
 - universiteiten en hogescholen
- voor onze software solutions maken we gebruik van onder andere
 - leveranciers van onderzoek software
 - universiteiten en hogescholen t.b.v. stages en projecten
 - leveranciers van hard- en software

backup

- Le Reseau is een 'kleine' organisatie en om continuïteit te garanderen hebben we onafhankelijke partners die in geval van nood als backup kunnen fungeren voor de dienstverlening van Le Reseau
- constructies van garantie van gelijkwaardigheid en tevens strikte vertrouwelijkheid van informatie (e.g. geheimhoudingsplicht)
- uiteraard wordt dit altijd in goed overleg vooraf besproken met onze opdrachtgevers, indien er een dergelijke situatie zich voordoet