ÖRYGGIS
MIÐSTÖÐIN

RAUNLÆGT ÖRYGGI

Ómar Rafn Halldórsson

VERÐMÆTAVERND

Þörfin á vernd verðmæta hefur fylgt okkur í gegn um árþúsundin, byggð á áhættumati

BÚNAÐUR TIL VARNA

Skiptast í:

Hindranir, töf og stýringu

- Ytri varnir
- Innri varnir

Greining og viðbragð

- Ytri varnir
- Innri varnir

HINDRUN, TÖF OG STÝRING

Náttúrulegar (í umhverfinu, manngerðar eða til staðar)

Girðingar: klifurhindranir, gaddavír, rafmagn

Veggir: steypa,málmur, timbur, gerviefni

Öryggisgler og filmur

Rimlar og málmgardínur

Hurðir og gluggar

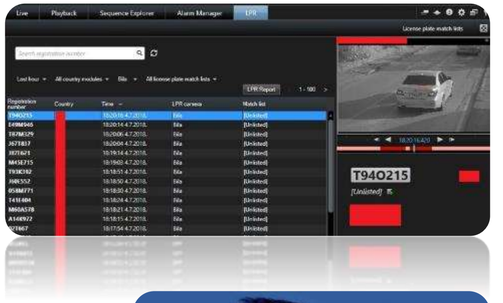
Tunnuhlið, þrífætur, slúsSur,

Hlið, bómur og pollar,

HINDRUN, TÖF OG STÝRING

Rafrænar aðgangsstýringar og kerfi

Kort og aðgangslyklar, snjallskilríki (mobile), öryggisnúmer,
fjarstýringar, raflæsingar, segullæsingar,
sjálfvirkar hurðalokanir
- aðgangsstýrðar hurðir eiga að vera lokaðar



Myndavélakerfi
Númeralestur, andlitsþekking, andlitsgreining, hvítlistun
inn á svæði, byggingar, rými

Vélrænar aðgangsstýringar

Lyklar og lyklakerfi, lásar, boltar, slagbrandar

HINDRUN, TÖF OG STÝRING

Líffræðileg einkenni:

- Andlitsgreining
- Fingraför
- Lófaför
- Lithimna
- Rödd

Samþætting lífkenna og annarra
aðgangsþátta s.s pin númer, kort eða
önnur aðgangsskilríki auka öryggisstig
til muna, tvöföld og jafnvel þreföld auðkenning

GREINING OG VIÐBRAGÐ

Eftirlitsmyndavélakerfi, (hitamyndavélar, hefðbundnar, AI)

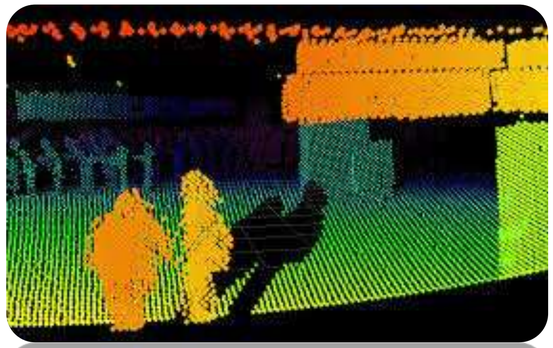
Örbylgjugirðingar

Laser-girðingar

Lidar skynjarar

Girðingaskynjarar

Hreyfiskynjarar, innrauðir og örbylgja



GREINING OG VIÐBRAGÐ

Eftirlitsradarar 360° eða stefnuvirkir

Titringsskynjarar í veggi og í jörðu

Öryggiskerfi

Hurðanemar

Eftirlitsdrónar

Eftirlitsvélmenni (autonomous-robotics)

ÁHÆTTUMAT, - FYRSTA SKREFIÐ

Áður en varnarbúnaður er settur upp eða verklagsreglur innleiddar er nauðsynlegt að framkvæma áhættumat.

- **Mat á virði upplýsingaeigna (** munnlegar, heyranlegar, sjónrænar, rafrænar**)**
- **Áhætta** sem hefur áhrif á þessar eignir hvað varðar ógnir og veikleika
- **Lögbundnar og lagalegar kröfur**
- **Núverandi mótvægisráðstafanir**
- **Hugsanlegir árásaraðilar**
- **Greining**

TRÚNAÐUR OG SAMÞYKKI

Auðkenning og staðfesting á notanda ásamt öryggis og **aðgangsstýringu** mynda saman venjulega burðarásvernd vegna trúnaðar gagna.

Almennt eru tvær meginástæður til að koma í veg fyrir aðgang að gögnum.

Skortur á aðgangsheimild

Mögulegur árásarmaður hefur ekki aðgangsheimild sem nauðsynleg er til að sjá upplýsingar sem verið er að nálgast.

Þarf að vita-þarf að hafa

Staða eða starfstitill er í sjálfu sér engin réttlæting fyrir því að einhver fái sjálfkrafa aðgang að gögnum, þótt viðkomandi hafi almennan og sértækan aðgang annarstaðar, þeir hafa aðgang þar sem þeir þurfa eftir mat hverju sinni.

MAT Á VIRÐI VARÐVEITTRA UPPLÝSINGA

Upplýsingainnviðir eru sambland af:

Vélbúnaði
Hugbúnaði
Gögnum
Net- og fjarskiptainnviðum
Starfsfólki

Þessa efnislegu og óefnislegu atriði sjáum við sem byggingareiningar, þegar þeir eru tengdir saman, mynda þeir innviði upplýsingakerfa okkar til að styðja við rekstur fyrirtækisins.

Mat á virði upplýsingainnviða ætti að skera úr um hvað er mikilvægt fyrir stofnun, eða fyrirtæki, og hvað þarf að vernda og hvers vegna?

ÁHÆTTA VEGNA ÓGNA OG VEIKLEIKA

Þegar við endurskoðum ógnir gagnvart starfseminni sem hluta af víðtækari öryggisstefnu þá þarf að fara fram svipuð endurskoðun sem beinist að ógnunum við upplýsingainnviði eins og t.d innbrot og skemmdarverk.

Þessi endurskoðun ætti einnig að bera kennsl á veikleika upplýsingainnviðanna, þ.e.a.s. fyrir hvaða árásum er upplýsingainnviðurinn berskjaldaður eða líklegur til að verða afhjúpaður.

LÖGBUNDNAR OG LAGALEGAR KRÖFUR

Lögboðnar og lagalegar kröfur sem settar eru á hvaða stofnun sem er eru mikilvægir þættir sem þarf að hafa í huga.

Þetta geta falið í sér viðbragðskröfur, aðgengi að upplýsingum eða viðbragðstíma. Allt þarf að vera tekið inn í heildaráhættumatið.

Staðlar lög og reglur varðandi geymslu og meðferð rafrænna upplýsinga eru til eftirfylgni.

NÚVERANDI MÓTVÆGISRÁÐSTAFANIR

Endurskoðun núverandi mótvægisaðgerða mun gefa upphafspunkt fyrir hvers kyns öryggisstefnu í framtíðinni.

Þessar mótvægisaðgerðir munu fela í sér:

- Stefna og verklagsreglur
- Núverandi öryggistækni uppsett
- Taktu öryggisafrit af ferlum og kerfum
- Viðbragðsfyrirkomulag, þ.m.t endurheimtusamningar

Sú vernd sem veitt er fyrir eignir sem ekki eru upplýsingar mun hafa bein áhrif á öryggi upplýsinga og ætti að vera óaðskiljanlegur hluti af upplýsingaverndaráætluninni

HUGSANLEGIR ÁRÁSARAÐILAR

Mikilvægt atriði er hugsanlegur árásaraðili sem getur - í hvaða tilgangi sem er, reynt að brjóta gegn öryggi upplýsinganna.

Hugsanlegur árásaraðili er hver sá sem er ekki viðurkenndur notandi gagna eða kerfis.

Í sumum tilfellum getur fólk verið hugsanlegur árásaraðili þó það hafi lögmætan aðgang t.d. ef þeir hafa einungis leyfi að sjá upplýsingar, en ekki breyta þeim.

HUGSANLEGIR ÁRÁSARAÐILAR

Eftirfarandi eru dæmi (í engri sérstakri röð)um hópa fólks sem gæti verið hugsanlegir árásaraðilar:

- Kerfisnotendur
- Viðhaldsstarfsfólk
- Ræstingin
- Fjölmiðlamenn
- Rannsakendur
- Þriðju aðila verktakar
- Erlendar leyniþjónustur eða umboðsmenn þeirra
- Hryðjuverkamenn
- Öfgafólk
- Samkeppnin

GREINING

Greining ætti að ákvarða mikilvægi eigna sem ætti að innihalda:

Áhrif öryggisbrots eða taps á upplýsingum
Tímann sem þarf að endurheimta upplýsingar eftir brot eða algjört tap
Lágmarksuppsetning og aðstaða sem þarf til að gera upplýsingar aðgengilegar eftir brot eða algert tap á upplýsingum.

Í kjölfarið ætti greiningin að ákvarða:
Vernd sem núverandi innviðirnir veita
Styrkleika innviða
Hverju er áfátt í öryggis- og viðbragðsfyrirkomulagi
Þarf að innleiða viðbótarfyrirkomulag til að mæta skorti?
Væntanlegur kostnaður og ávinningur af valkostunum
Tæknileg vandamál sem hafa áhrif á hvern valkost
Hugsanleg áhrif þess að setja ekki upp hvern valkost

GREINING

Verndun eigna er grundvallarkrafa.

Upplýsingar eru slík eign og kerfi tengd þeim , þau eru mikilvægur þáttur í áætlun um verndun eigna fyrirtækisins.

Öryggi upplýsinga þarf að nálgast á heildrænan hátt, þar sem allt sem þarf að vernda þarf að bera kennsl á og meta út frá heildaráhættustýringu

GÆÐAHANDBÓKIN

er lifandi skjal

Hún inniheldur:

Áhættumat
Verklagsreglur og ferla
Viðbragðsáætlun (Business Continuity Plan)
Hlutverk hvers og eins
Tengiliði og símanúmer
Dagbók

ÖRYGGIS MIÐSTÖÐIN

TAKK FYRIR