SKYDD FRÅN INSIDERHOT

EN GUIDE TILL STÄRKT FÖRMÅGA ATT SKYDDA VERKSAMHETEN MOT INSIDERHOT,
PRESENTERAD AV SPALDING SECURITY SOLUTIONS OCH REKYL.

REKYL PODDEN

REKYL | IN OMNIA PARATUS®

SPALDING
SECURITY SOLUTIONS

SKYDD FRÅN INSIDERHOT

EN GUIDE TILL STÄRKT FÖRMÅGA ATT SKYDDA VERKSAMHETEN MOT INSIDERHOT, PRESENTERAD AV SPALDING SECURITY SOLUTIONS OCH REKYL. *

REKYL PODDEN

REKYL | IN OMNIA PARATUS®

SPALDING SECURITY SOLUTIONS

ATTACKVEKTORER

- Dysfunktionell organisation
- Karaktärsdrag
- Extern antagonist

KULTUR

(Grunden för att arbeta med insider risk)

LEDARSKAP

- Säkerhetskultur börjar med GD/VD + ledningsgruppen
- Synliggör säkerhetspolicy
- Tydliggör hur det ska genomföras
- Har en ”öppen-dörr policy”
- Synliggör medarbetarna
- Skapa engagemang för huvuduppgiften

KOLLEKTIV SÄKERHETSMEDVETENHET

- Utbildning och kommunikation sprider kunskap och förståelse
- Rätt förutsättningar ger förväntningar vilket leder till aktivt deltagande i säkerhetsarbetet

INSIDERHOT

- ORSAKER OCH INDIKATORER

KARAKTÄRSDRAG

- Förbittring/missnöje
- Bristande social kompetens
- Missbruk
- Psykiatrisk störning, grandios självbild etc.

STRESSORER/TRIGGERS

- Bristande ledarskap
- Finansiell situation
- Förändringar i privatlivet
- Förändringar i jobbsituation

BETEENDE

- Kränkande eller offensiva kommentarer på lunchen eller fikat.
- Kort stubin, hett temperament, aggressivitet
- Ökande konflikter med medarbetare
- Slutar tidrapportera eller leverera i projekt
- Jobbar sent, eller tidiga mornar
- Börjar sluta sig och pratar mindre om sina intressen
- Slutar reserapportera, även när det är känt att han/hon rest

TEKNISKA INDIKATORER

- Skriver ut känsliga dokument
- Tar med sig känsliga dokument hem
- Överför dokument till extern lagring/ cloudlösningar
- Jobbar mer hemifrån mer frekvent
- Försöker komma åt avlysta områden som inte besökts tidigare

DYSFUNKTIONELL ORGANISATIORISK RESPONS

- Organisationen kan inte/vill inte ta tag i problem, är inte rustad med verktyg för att handskas med uppkomna tecken på potentiella insiderhandlingar (Strutsmentaliteten)

VERKTYGEN

- Multidisciplinära engagemanget: Säk+HR+Ledning+Juridik+Fyssäk+ Infosäk+IT/Cyber+Compliance
- Etablerad säkerhetskultur
- Tekniska lösningar för att upptäcka avvikelser - som kompletterar magkänsla
- Handlingsplan för hur organisationen ska agera innan det blir ett hot och när det redan är ett hot: Insider Risk/Threat Mitigation Program

*Den här sammanställningen är inte fullständig. Det finns fler ingredienser för att stärka upp säkerheten i en organisation, t.ex cybersäkerhet och skalskydd.

Lyssna på RekylPoddens avsnitt med Anders Spalding:

https://open.spotify.com/episode/5k24LKSnIBwb-SUOThca4EJ?si=fd41f4a-849e7458f

MER ATT LADDA HEM:
Ett stort urval av gratis nedladdningsbart material i form av guider och handböcker inom ramen för handlingsplaner för Insider Risk finns hos CISA.

https://www.cisa.gov/topics/physical-security/insider-threat-mitigation

Källa: Shaw & Sellers, (2015). Application of the Critical-Path Method to Evaluate Insider Risks, Studies in Intelligence, Vol. 59, No.2, pp. 1-16.