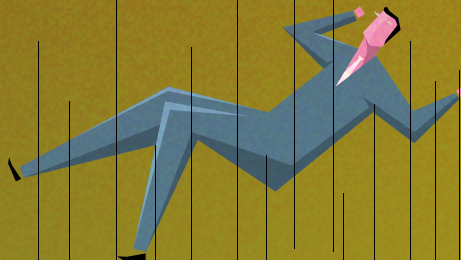




VSSE

veiligheid van de staat
sûreté de l'état



WORDT U GEVISEERD?

Spionage en inmenging
Overheidsdiensten - Diplomatie

Spionage en inmenging zijn ernstige bedreigingen. Buitenlandse mogelijkheden zetten de meest uiteenlopende middelen in, waaronder spionage, om informatie te verkrijgen die niet publiek toegankelijk is. Via inmenging proberen ze ook beslissingsprocessen te beïnvloeden.

Medewerkers en vertegenwoordigers van een overheidsdienst vormen een interessant doelwit voor dit soort activiteiten. Dat impliceert dat u een essentiële schakel bent voor de veiligheid van onze instellingen en onze democratische processen.

Hoe kan u zich tegen spionage en inmenging beschermen? De eerste stap bestaat erin deze dreigingen te begrijpen en ze te herkennen. Met deze brochure wil de Veiligheid van de Staat u helpen om uw weerbaarheid en die van uw organisatie te versterken.



WAAROVER



GAAT HET?

Spionage en inmenging zijn dreigingen die per definitie weinig zichtbaar zijn. Op een misleidende of clandestiene manier worden inlichtingen verzameld of wordt invloed uitgeoefend, bijvoorbeeld door mensen te manipuleren of communicatie te onderscheppen.

Hierdoor wordt een onrechtmatig voordeel verworven dat vervolgens kan worden misbruikt bij diplomatieke of commerciële onderhandelingen. Zo kunnen nationale bedrijven van deze landen worden bevoordeeld of omgekeerd, kan een tegenstander of een geostrategische concurrent worden gedestabiliseerd.

Sommige staten gebruiken spionage en inmenging ook als een middel om controle uit te oefenen of om vat te krijgen op hun gemeenschappen (diaspora) in ons land.

Dergelijke methodes worden vooral ingezet door buitenlandse inlichtingendiensten, hun agenten of hun bondgenoten. Het gaat dan niet alleen om Rusland of China: tal van buitenlandse mogendheden maken er gebruik van.

HOE WERKT HET?



Buitenlandse inlichtingendiensten werken zeer discreet en maken gebruik van dekmantels. Hun spionnen doen zich voor als diplomaat, journalist, ambtenaar, lobbyist, onderzoeker, professor of eender welke andere functie, zolang die maar legitiem of geloofwaardig genoeg is om met u in contact te kunnen treden. België telt zo honderden buitenlandse inlichtingenofficieren die werken onder een dekmantel. Daarnaast hebben ze ook nog een netwerk van contacten en agenten waar ze een beroep op kunnen doen.

Ze exploiteren voornamelijk onze persoonlijke kwetsbaarheden en de onvolmaaktheden in de elektronische toestellen die we elke dag gebruiken.

De manier waarop mensen gemanipuleerd worden, kan zeer uiteenlopende vormen aannemen. Het kan gaan om een professionele of vriendschappelijke relatie waar een verborgen agenda achter schuilt, verstopt achter een façade van hoffelijkheid, gedeelde ideologische of culturele referenties en vleierijen. Dit type van relatie is doorgaans asymmetrisch: meestal neemt uw gesprekspartner het initiatief bij de contacten en toont hij zich altijd genereus en dienstbaar. Deze schijnbaar aangename en onschuldige handelingen dienen om een klimaat van vertrouwen te scheppen. Zo ontstaat een nauwe vriendschapsband met ruimte voor vertrouwelijkheid en wederzijdse hulp. Deze valse vriendschap is de voedingsbodem voor manipulatie.

Enkele voorbeelden

Voorbeeld 1. Een persoon die u ontmoet hebt op een evenement, nodigt u uit op restaurant. Het klikt en u ontmoet elkaar meer dan een keer. Door de vriendschap die ontstaat, vermindert uw waakzaamheid en u begint uw indrukken en allerlei roddels over de leden van het directiecomité te delen.

Behalve manipulatie van mensen komt ook technische spionage vaker voor, en dit als gevolg van onze toenemende afhankelijkheid van digitale technologieën en mobiele toestellen.

Voorbeeld 2. U heeft op een link geklikt die u betrouwbaar leek en heeft de instructies gevolgd: voer login/wachtwoord in van uw professionele account. De gegevens worden vervolgens gebruikt om binnen te dringen in het netwerk van uw organisatie.



ALLE BELEIDSNIVEAUS ZIJN BETROKKEN

Naargelang hun strategische doelstellingen zijn buitenlandse inlichtingendiensten geïnteresseerd in elke instantie die relevante informatie verstrekt, verzamelt of coördineert en dat in de meest uiteenlopende domeinen.

Het gaat logischerwijs om diplomatieke of economische belangen, maar ook om talloze andere domeinen zoals onderzoek, innovatie, investeringen, media, immigratie, religieuze aangelegenheden, enz. Ook gecentraliseerde databanken (Rijksregister, DIV, RIZIV, KSZ, enz.) Én degenen die er toegang toe hebben, kunnen een doelwit vormen.

ALLE INFORMATIE IS WAARDEVOL

Spionage beperkt zich niet tot de diefstal van vertrouwelijke of geheime documenten. De werkwijze is veeleer vergelijkbaar met een puzzel, waarvan elk onderdeel een extra element vormt dat tegen uw belangen kan worden ingezet. Informatie over de interne werking van uw organisatie, haar structuur, de persoonlijke problemen en belangen alsook de interpersoonlijke relaties of zelfs gewoon de contactgegevens kunnen buitenlandse spionnen interesseren. Deze gegevens kunnen bijvoorbeeld dienen om de meer kwetsbare personen te identificeren of uw organisatie te beschadigen.

HOE KAN U ZICH BESCHERMEN?

Om u te beschermen, is het van het grootste belang dat u zich bewust bent van uw kwetsbaarheden en dat u zich - zowel individueel als collectief - zoveel mogelijk beschermt.

UW MEDEWERKERS EN UW COLLEGA'S SENSIBILISEREN IS DAARBIJ EEN ESSENTIËLE EERSTE STAP.

Ook al zijn de gevolgen niet altijd zichtbaar, het is belangrijk te begrijpen dat de dreiging reëel is. Aarzel dan ook niet om deze brochure binnen uw organisatie te verspreiden en contacteer de Veiligheid van de Staat indien u bijkomende informatie wenst.

Daarnaast is het ook belangrijk om (preventieve) veiligheidsmaatregelen te treffen. Dat betekent de risico's beperken door een zo ruim en krachtig mogelijke veiligheidspolitiek te voeren en met andere woorden, de blootstelling aan de dreiging te beperken alsook de mogelijke impact. Wees weerbaar!



AANDACHTSPUNTEN

Frustratie leidt tot manipulatie

Offensieve inlichtingendiensten zijn gespecialiseerd in het manipuleren van mensen. Ze spelen in op de kwetsbaarheden en de frustraties van individuen. Gebrek aan erkenning, toenemende rancune of onopgeloste functioneringsproblemen vormen een ideale voedingsbodem voor manipulatie. Vandaar dat een gezond en zorgzaam personeelsbeleid een essentieel element is om dit soort frustraties te voorkomen.

Need-to-know

Zorg ervoor dat de toegang tot de meest gevoelige gegevens uitsluitend is voorbehouden aan personeelsleden die deze nodig hebben in het kader van hun dagelijks werk. Door het need-to-know-principe te hanteren, zal u het risico op misbruik van deze informatie beperken. Een procedure voor het adequaat vernietigen van gevoelige informatie verzekert bovendien een betere bescherming van de vertrouwelijkheid.



Wees discreet

Consulteer of bespreek geen gevoelige informatie op openbare plaatsen. Iemand kan van de gelegenheid gebruik maken om er kennis van te nemen zonder dat u het weet. Kwaadwillig of gewoonweg ongepast gebruik van dergelijke informatie kan uw organisatie schade toebrengen.



Altijd bereikbaar = altijd traceerbaar

Smartphones maken ons het leven makkelijker, en ook dat van de inlichtingendiensten. Hoogtechnologische, schadelijke programma's kunnen echter uw gegevens onderscheppen of uw toestel aanvallen. Hou uw besturingssysteem en apps daarom up-to-date en gebruik sterke identificatieprocedures. Gebruik bij de opslag van of toegang tot gevoelige gegevens op uw smartphone encryptiesoftware en een VPN-verbinding. Het is ook sterk aanbevolen om voor buitenlandse dienstreizen een afzonderlijk toestel te gebruiken.



Reizen naar het buitenland

Buiten onze grenzen zijn we kwetsbaarder en de offensieve diensten staan er sterker. Reizen vormen een uitgelezen kans voor spionage. Het is dus noodzakelijk om bijkomende voorzorgen te treffen. De kernwoorden daarbij zijn: voorzichtigheid en discretie. Verlaag het risico door het aantal documenten tot het strikte minimum te beperken en uw datadragers te beveiligen. Aanbevelingen hieromtrent vindt u in de brochure "Travel Security" op onze website

www.vsse.be





Sociale media

Offensieve diensten gebruiken ook de nieuwe mogelijkheden van de sociale media. Deze platformen maken het makkelijker om potentiële doelwitten in kaart te brengen en ze vermenigvuldigen ook de potentiële contacten. Wees zeker dat u de persoon kent vooraleer u een “vriend” of een virtueel contact van hem/haar wordt. Denk er ook aan dat elk nieuw contact dat u aanvaardt, toegang krijgt tot uw kring van virtuele relaties. Dit geeft hen een niet te verwaarlozen extra legitimiteit en kan latere pogingen tot manipulatie vergemakkelijken.

Controle, verificatie en habilitatie

Zorg voor een allesomvattende controle- en toegangspolitiek zonder naïef of paranoïde te worden. Bezoekers moeten van tevoren geïdentificeerd worden en kunnen zich best niet zonder begeleiding verplaatsen binnen uw gebouw noch toegang krijgen tot het interne netwerk van uw organisatie. Bepaalde lokalen moeten bovendien voorbehouden blijven voor medewerkers met een specifieke functie. Voor sommige lokalen moet de toegang zelfs beperkt worden tot personen met een veiligheidsmachtiging of -verificatie (op basis van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen).



Bezoek van buitenlandse delegaties

Het bezoek van een buitenlandse delegatie is de gelegenheid bij uitstek om relaties aan te knopen of een nuttige samenwerking uit te bouwen. Voor buitenlandse inlichtingendiensten is het ook de kans om niet-publieke informatie in te winnen of om relaties op te bouwen met het oog op spionage of inmenging. Sociaal-culturele activiteiten lenen zich perfect tot informele contacten, die helaas niet altijd wenselijk zijn. Wees daarom op uw hoede en zorg ervoor dat de betrokken medewerkers over alle nodige informatie beschikken om de grenzen van bepaalde contacten correct te kunnen inschatten.

SLACHTOFFER VAN SPIONAGE OF INMENGING?

WAT TE DOEN?

Als u denkt dat u of uw organisatie het slachtoffer is geworden van spionage- of inmengingsactiviteiten, contacteer dan de veiligheidsverantwoordelijke van uw organisatie of de Veiligheid van de Staat (VSSE). Het is nooit te laat om te melden, maar probeer het onderzoek vooral niet op eigen houtje te voeren.

De VSSE inlichten is in het belang van iedereen. U zal op onze discretie en op onze steun kunnen rekenen. Dankzij uw samenwerking zullen we de fundamentele belangen van ons land nog beter kunnen beschermen.



MEER

INFORMATIE ?

Raadpleeg onze website : www.vsse.be



Veiligheid van de Staat (VSSE)
Koning Albert II-laan 6 - 1000 Brussel

+32 (0) 2 205 62 11
info@vsse.be

