SSSST! De muren hebben oren en ogen! Computers ook.

Bescherm de intelligentie en kennis van uw bedrijf!

Uw materiële activa beschermen tegen brand, kwaadwillige daden of natuurrampen volstaat niet om de economische toekomst van uw onderneming veilig te stellen. Iedereen denkt aan schade aan gebouwen, apparatuur, opslag en productieprocessen, maar niet-financiële en "immateriële" risico's kunnen net zo zwaar wegen op het voortbestaan van een onderneming. Of het nu gaat om een grote groep, een start-up, een kleine of middelgrote onderneming (kmo) of zelfs een onderzoeksinstantie, ze worden allemaal blootgesteld aan het verlies van gegevens of onderzoeksresultaten of aan de ongecontroleerde verspreiding van hun knowhow.

Goed beheer houdt in dat alle economische, technologische en wetenschappelijke activa van de onderneming of organisatie worden beschermd om het risico van buitmaking, verspreiding en frauduleus of kwaadwillig gebruik te beperken. Wat zijn de gevolgen van diefstal of verlies van gegevens, octrooien, intellectuele eigendom, diefstal door een externe kwaadwillende partij, een concurrent of vijandige kandidaat-investeerder?

Dergelijke gegevens of informatie circuleren in de vorm van "geruchten" of zelfs persberichten. Door een zorgvuldige monitoring kunnen ze worden opgespoord en kan worden gereageerd om de situatie recht te zetten. Het is beter ze te vermijden en de mogelijke bronnen weg te werken. Is het gewoon loos geklets of een slecht geregisseerd interview, het antwoord op een onrechtmatige vraag van buitenstaanders?

Het beheer van interne en externe informatie is de hoeksteen van elk beleid ter bescherming van uw technologische, economische en financiële kennis.

EEN GECOÖRDINEERD INFORMATIEBEHEERSPLAN

De economische veiligheid kan niet beperkt blijven tot enkele ad hoc technische of organisatorische maatregelen. De doeltreffendheid ervan hangt af van de uitvoering van een echt beleid ter bescherming van de belangen, de knowhow en het informatiekapitaal – net zoals het globale plan voor preventie en veiligheid op het werk, of voor brandpreventie.

Het plan is gebaseerd op elementaire organisatorische en gedragsmaatregelen, waarbij voor elk risico of elke kwetsbaarheid een specifiek actieplan en specifieke procedures worden opgesteld.

Organisatorische maatregelen:
- Een algemene diagnose opstellen met identificatie van de risico's, bedreigingen en kwetsbaarheden.
- De nodige menselijke, financiële, materiële middelen enz. toewijzen.
- Een verantwoordelijke voor de veiligheid en beveiliging van de informatiesystemen aanduiden.
- Alle personeelsleden betrekken via de juiste procedures.
- Prioritaire doelstellingen vastleggen en toezien op de verwezenlijking ervan door middel van audits en prestatie-indicatoren.
- Het personeel voorzien van eenvoudig, toegankelijk en up-to-date communicatie- en bewustmakingsmateriaal.
- Bewustmakings- en opleidingsactiviteiten organiseren, aangepast aan elke afdeling of dienst.
- Een regelmatige dialoog organiseren tussen de verantwoordelijken voor de veiligheid/business intelligence en het kaderpersoneel.

Gedragsmaatregelen:
- Toegankelijk zijn en reageren op alle veiligheidsvragen die intern worden gesteld.
- Nooit het belang van een ongewoon voorval of een veiligheidsincident onderschatten.
- Elk ongewoon voorval of incident aan de verantwoordelijke melden.

VASTSTELLEN WELKE GEGEVENS EN INFORMATIE PRIORITAIR MOETEN WORDEN BESCHERMD

De vele informatiebronnen die in een onderneming beschikbaar zijn, kunnen niet op dezelfde manier worden gecontroleerd want dat zou verlammend werken. Bij een analyse moet eerst worden vastgesteld welke informatiebronnen en soorten informatie (gegevens) werkelijk van essentieel belang zijn, ongeacht of zij intern worden geproduceerd of afkomstig zijn van derden (leveranciers, klanten, financiële partners enz.).

Organisatorische maatregelen:
In overleg met het hele managementteam – alle diensten of afdelingen zijn erbij betrokken:
- de soorten aanwezige gegevens/informatie verzamelen en identificeren;
- de gevoeligheid van de informatie bepalen op basis van de potentiële schade voor het bedrijf (lage, middelmatige, hoge impact) in geval van openbaarmaking, verlies of vernietiging.

  Vragen die men zich moet stellen:
  Bestaat de kans dat het verlies, de vernietiging of de openbaarmaking van deze informatie zal leiden tot ...:
  - ... schade aan de betreffende activiteit of de voortgang van een project?
  - ... een financiële of technische impact?
  - ... een impact op het personeel?
  - ... een impact op het vlak van imago en reputatie?
  - ... een impact op het vertrouwen van de aandeelhouders of de banken?
  - ... minder vertrouwen van een klant of een belangrijke partner?
  - enz.

- de frequentie waarmee het risico zich voordoet evalueren, en de menselijke of technische impact ervan specificeren.

  Vragen die men zich moet stellen:
  - Wie heeft toegang tot deze informatie – intern en extern?
  - Zijn de toegangsrechten tot de informatie geregeld (zeer beperkt, beperkt, vrij)?
  - Hoe wordt deze informatie opgeslagen? Wordt ze regelmatig geback-upt?
  - Moet de informatie op een digitale of andere drager worden getransporteerd?
  - Hoe verloopt de uitwisseling van informatie?
  - enz.

- de resultaten analyseren en volgens het potentiële risiconiveau in een tabel gieten;
- op elk type gegevens de beschermingsmaatregelen toepassen die in het informatiebeheersplan zijn omschreven (toegang, verspreiding, vermenigvuldiging, archivering, vernietiging enz.). De gevoeligste informatie moet extra worden beschermd.
- de analyse en voorgenomen beschermingsmaatregelen regelmatig evalueren en bijwerken;
- Deze aanpak wordt ook toegepast bij andere preventie- en veiligheidsprocedures in geval van rampen (brand, overstroming, natuurramp enz.).

Tabel 1: Voorbeeld van een rooster om de kriticiteit te evalueren

			IMPACT / ERNST				
			Catastrofaal	Ernstig	Matig	Gering	Onbeduidend
			5	4	3	2	1
WAARSCHIJNLIJKHEID / FREQUENTIE	Heel sterk	5					
	Sterk	4					
	Gemiddeld	3					
	Laag	2					
	laag	1					

RISICOBEOORDELING:

- Rood: te hoog risiconiveau. Het risico wordt geacht te groot te zijn en de beheersing ervan is problematisch. Het risico moet tot een aanvaardbaar niveau worden teruggebracht door aanvullende beperkingsvoorstellen te formuleren, zoals een aangepast beschermingsplan om uit de rode zone te komen, in combinatie met maatregelen voor informatiebeheer (toegang, verspreiding, vermenigvuldiging, archivering, vernietiging enz.). De meest kritieke informatie moet altijd extra worden beschermd;
- Geel: hoog risiconiveau. Het risico moet tot een lager niveau worden teruggebracht;
- Groen: gemiddeld risiconiveau. De risicobeheersingsmaatregelen zouden moeten volstaan. Een aanpak van voortdurende verbetering blijft echter relevant om, onder economisch aanvaardbare voorwaarden, een zo laag mogelijk risiconiveau te bereiken;
- Grijs: lager risiconiveau.

Bron: La sécurité économique au quotidien – zie referenties aan het einde van het artikel

PAPIEREN EN DIGITALE ARCHIEVEN BEHEREN

Net als levende documenten zijn archieven bronnen van informatie voor wie technische, commerciële of menselijke informatie over uw activiteiten zoekt.
Naast de verplichte archieven verdienen ook andere documentvormen zoals handgeschreven notities, e-mails, digitale bestanden, overzichten, verslagen en samenvattingen uw aandacht en beschermingsmaatregelen.

Organisatorische maatregelen:
- klasserings- en archiveringsplan voor documenten waarvan de inhoud als gevoelig wordt beschouwd;
- opleiding van het personeel in het beheer en de beveiliging van back-ups van documenten (gevoeligheidsniveau, levensduur);
- procedure voor monitoring en tracering van de raadpleging van de verschillende gearchiveerde documenten;
- uitbesteding van digitale archieven – contractueel vastleggen van de voorwaarden voor verwerking en openbaarmaking aan de verschillende partners;
  - specifieke voorwaarden en clausules die voorzien in de opslag en/of veilige vernietiging van harde schijven, IT-apparatuur (server, computer, printer, faxapparaat, tablet enz.).

Opmerking:
Maak het personeel in het licht van de huidige mogelijkheden van telewerk bewust van het gevaar van eigen opslagmedia. Het is beter om ze te verbieden en door u geverifieerde media aan te bieden en te beheren.

Technische maatregelen:
- veilige en geschikte ruimten voor de opslag van papieren documenten en digitale media (toegangscontrole, binnenklimaat (vochtigheid, temperatuur, ventilatie), geschikte brandbeveiligingssystemen, bescherming tegen overstromingen, afhankelijk van de conclusies van de risicoanalyse);
- de gevoeligste gegevens worden apart opgeslagen in een kluis. Kopieën en back-ups worden op afzonderlijke locaties bewaard;
- een cross-cut versnipperaar ter beschikking stellen om gevoelige documenten
- (papieren, cd, dvd enz.) veilig te vernietigen.

Zorgen voor de veilige vernietiging van documenten:
- een cross-cut versnipperaar voorzien om gevoelige informatiedragers te vernietigen (papier, cd, dvd enz.);
- gevoelige documenten (papier, cd, dvd enz.);
- werkstations uitrusten met software voor veilig wissen;
- het interne geheugen van de IT-apparatuur veilig vernietigen aan het einde van hun levensduur of aan het einde van het contract (printer, fax, fotokopieerapparaat enz.);

© VZ_Art / Adobe Stock

- veilig vernietigen van afgedankte prototypes en restanten van innovatieve materialen.

HET VERZAMELEN VAN DE INFORMATIE EN DE COMMUNICATIE BEHEERSEN

Beheersing van de informatie impliceert beheersing van de communicatie. Slecht beheerste communicatie kan leiden tot het uitlekken van strategische en nadelige informatie. De gevoeligheid van de gecommuniceerde informatie moet altijd intern en extern worden beoordeeld op professioneel of persoonlijk niveau. Deze beheersing impliceert de invoering van een structuur en de duidelijke omschrijving van de taken en verantwoordelijkheden van de verschillende partijen die betrokken zijn bij de communicatiecellen binnen de organisatie.

Organisatorische maatregelen:
- communicatie moet gestuurd worden:
  - welke functie(s) of perso(o)n(en) is (zijn) bevoegd om te spreken en te communiceren naar gelang van het soort communicatie of informatie?
- communicatie moet beheerst worden:
  - evalueren of de aanvraag voor een bezoek of een interview legitiem is en strookt met de bedrijfs- of communicatiestrategie van de onderneming;
  - de directie en/of de communicatieverantwoordelijke vooraf op de hoogte brengen van elk verzoek om contact met de media (pers, of redacteur van een website of sociale media). Sommige verzoeken kunnen ook komen van bijvoorbeeld analisten, onderzoekers of concurrenten. Zijn de contactpersonen legitiem?
  - het onderwerp en het doel van het bezoek of interview laten verduidelijken. Indien mogelijk verzoeken

om de vragen vooraf te kennen en zorgen dat u de tekst vóór publicatie mag nalezen;
  - niet alleen de positieve maar ook de negatieve gevolgen van de verstrekte informatie (mondeling of schriftelijk) afwegen.
- de boodschappen voor verspreiding tijdens evenementen voorbereiden (beurzen, conferenties, productlanceringen, symposia enz.);
  - de doelstellingen vastleggen en doorgeven aan uw medewerkers;
  - gevoelige informatie identificeren en vragen buiten de context ontwijken;
  - alleen informatie communiceren die relevant is voor het bedrijf, de doelstellingen of de professionele relaties;
- persoonlijke gegevens op visitekaartjes, in elektronische handtekeningen enz. beperken tot wat strikt noodzakelijk is;
- werknemers bewustmaken van de risico's van vragen die dringend, ongewoon of in strijd met de procedures zijn. Deze kunnen een slinkse manier zijn om gevoelige informatie te verkrijgen. Een noodprocedure voorzien;
- een door het bedrijf goedgekeurde noodcommunicatieprocedure opstellen om de reactie op een negatief of ongepast bericht in goede banen te leiden;
- de legitimiteit van audits, controles, reparateurs of bezoekers die toegang moeten hebben tot vertrouwelijke of gevoelige gegevens controleren:
  - de identiteit van de betreffende personen controleren bij de administraties, controle-instanties of leveranciers waartoe zij beweren te behoren;
  - vooraf een afspraak maken, vragen naar de beroepskaart, ...;
  - een opdrachtbevestiging eisen.
- waken over de reputatie van de onderneming:
  - controleren wat er gezegd of geschreven wordt over uw bedrijf, zijn managers of werknemers.
  - De belangrijkste media en sociale netwerken regelmatig in de gaten houden;
  - altijd eensgezind reageren op laster, "cyberaanvallen" of andere kritiek op het bedrijf;
  - de informatie corrigeren en proberen de bron te achterhalen.

Jeanine DRIESSENS
ANPI - Information & Media Center

Bron: Dit artikel is grotendeels geïnspireerd op:
"La sécurité économique au quotidien" - Ministère de l'économie et des finances et de la relance (Frankrijk) - Service de l'information stratégique et de la sécurité économiques (Sisse) - Direction générale des Entreprises (DGE) / November 2021
Fiches A1, A3, C3 en F1

© Thapana_Studio / Adobe Stock