|  |  |  |  |
| --- | --- | --- | --- |
| Titel : Waartegen moet je je beveiligen | | | |
| Kerntaak | Keuzedelen | Duur | ….. dagdelen |
| Werkproces | Security | Opleiding | BOL |
| Opdrachtcode | 2. Waartegen moet je je beveiligen. | Niveau | 3/4 |

In deze opdracht behandelen we:

* Wat men onder security verstaat;
* Welke security maatregelen er zijn;
* Welke organisatorische security maatregelen er zijn;
* Wat men onder personele security maatregelen verstaat;
* Welke fysieke security maatregelen kunt nemen;
* Wat men onder ICT-security maatregelen verstaat.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Inleiding**  Veiligheid (safety) en beveiliging (security) zijn tegenwoordig niet meer weg te denken binnen bedrijven en ook daar buiten. Logisch, de belangen van de bedrijven zijn groot en er zijn veel (be)dreigingen die de belangen kunnen schaden.  De vraag doet zich voor hoe bedrijven zich tegen deze (be)dreigingen kunnen beschermen. Dit ‘beschermen ’of ‘beveiligen’ duidt men in vaktaal veelal aan met security.  Een computer zonder beveiliging is als een huis zonder slot op de deur. Voor zowel eenmanszaken als ondernemingen met personeel zijn een antivirusprogramma en firewall minimale veiligheidseisen. Voor een complete beveiliging is meer nodig.  **Opdracht 1**   * Lees de tekst “Security maatregelen“ goed door. * Beantwoord de volgende vragen: * Veel kledingwinkels en warenhuizen hebben te maken met diefstal. Welke security maatregelen gebruiken deze winkels?   **Elektronische maatregelen zoals poortjes bij de uitgang**   * Security maatregelen worden verdeeld in groepen. Welke groepen zijn dit?   **organisatorische security maatregelen;**  **personele security maatregelen;**  **bouwkundige security maatregelen;**  **elektronische security maatregelen;**  **ICT-security maatregelen.**  Security maatregelen  Security heeft tot doel de belangen van een bedrijf te beschermen tegen onbevoegde en/of onbedoelde beïnvloeding. Daaronder valt ook het moedwillig verstoren van de bedrijfsprocessen.  De security doelen voor bedrijven in de vitale infrastructuur, kennen de volgende volgordelijkheid:   * Voorkomen dat gevoelige of kwetsbare informatie in het publieke domein terecht komt (bijvoorbeeld op het internet). * Afschermen van aantrekkelijke en kwetsbare onderdelen om kennisname en verkenningsacties door kwaadwillenden te bemoeilijken. * Afschrikken van kwaadwillenden. De kwaadwillende moet het gevoel hebben dat de beveiliging bij het bedrijf goed op orde is. * Tegenhouden. De kwaadwillende wordt het fysiek onmogelijk gemaakt zijn daad te verrichten. * Detectie. Indien al het voorgaande de kwaadwillende niet heeft afgeschrikt of tegengehouden, is het zaak zijn inbreuk zo vroeg mogelijk te detecteren. * Vertragen. Het opwerpen van barrières tussen de gedetecteerde kwaadwillende en zijn doel. Dit kan zowel het binnendringen als het kunnen vluchten betreffen. * Interventie. De kwaadwillende wordt tijdig door een bevoegde en capabele functionaris tegengehouden. Uitlevering aan Justitie behoort tot de mogelijkheden.   Om deze doelen te bereiken staan ons meerdere security strategieën, security maatregelen en voorzieningen ter beschikking.  Bij security management worden security maatregelen verdeeld in groepen. Daarbij komt men veel verdelingen tegen. Een veel toegepaste verdeling is de volgende verdeling:   * organisatorische security maatregelen; * personele security maatregelen; * bouwkundige security maatregelen; * elektronische security maatregelen; * ICT-security maatregelen.   Met in het achterhoofd het bedrijfsbeleid zal de security manager zich op het gebied van security tot doel moeten stellen deze maatregelen en voorzieningen kosteneffectief te realiseren. De manager zal dus die maatregelen en voorzieningen moeten kiezen  waarmee het vereiste security niveau daadwerkelijk te realiseren is tegen zo gering mogelijke kosten.  **Opdracht 2**   * Onderzoek welke beveiligingsmaatregelen er zijn of worden genomen bij de Haagse ministeries?   **ICT, elektronische, personele, bouwkundige**   * Hieronder staat een lijst met voorbeelden van organisatorische security maatregelen. Welke zijn van toepassing bij een bank? En welke bij een museum?   **Toegangsbeheer, zoneringsplan, fotografeerverbod( voor bepaalde gedeelten) sluitplan, autorisatie, clean desk regeling, rubriceringsregeling, merkingsregeling, registratie en archivering, procedure alarmopvolging, incidentenregistratie opleidingsplan security, communicatieplan**  Organisatorische security maatregelen  De meest verstrekkende maatregelen zijn de organisatorische maatregelen. Deze vormen de basis voor de security van het bedrijf. Het vergt niet alleen veel denk- en schrijfwerk, vooral de naleving van deze maatregelen vergt de nodige aandacht.  Daarnaast hangt de consistentie van de beveiliging af van de kwaliteit van de organisatorische maatregelen. Een goede veiligheidscultuur draagt positief bij aan de kwaliteit van de security en het borgen daarvan. Veiligheidsbewustwordingsprogramma’s  kunnen de veiligheidscultuur verbeteren.  Voorbeelden van organisatorische maatregelen zijn:   * toegangsbeheer; * zoneringsplan (wie mag waar komen?); * fotografeerverbod; * sluitplan (waaronder sleutelbeheer); * autorisatie toekenning en autorisatiebeheer (wie mag wat?); * uitvoerbeleid (geautoriseerd meenemen van bedrijfseigendommen); * clean desk regeling (wat moet altijd worden opgeborgen?); * need-to-know regeling (wie mag wat weten?); * rubriceringsregeling (personeelsvertrouwelijke informatie, patentinfo etc.); * merkingsregeling (markeren en registreren van waardevolle assets); * registratie en archivering (van kwetsbare informatie); * procedure alarmopvolging (detectie en tijdpadanalyse); * incidentenregistratie; * opleidingsplan op terrein van security; * communicatieplan op terrein van security (o.a. veiligheidsbewustzijn).   **Opdracht 3**   * Wat is een VOG?   **Verklaring omtrent gedrag**   * Zoek uit bij welke beroepen een VOG noodzakelijk is en waarom?.   **werk met vertrouwelijke gegevens, kwetsbare personen, geld of goederen.**   * Hoe kom je aan een VOG?   **Kan je opvragen bij de overheid**   * Wanneer je gaat solliciteren moet je soms referenties opgeven of noemen tijdens je sollicitatiegesprek. Bedenk een aantal redenen waarom een potentiële werkgever om referenties zou vragen.   **Zodat diegene weet hoe jij bent en werkt en gewerkt heb**   * Vele beroepen kennen de geheimhoudingsplicht. Is dit ook van toepassing op het beroep ICT-er? Licht je antwoord toe.   **Ja want wij kunnen bij vertrouwelijke informatie komen**   * Wanneer een werknemer uitdienst treedt, beschikken veel bedrijven over een procedure “Uitdiensttreding”. Welke maatregelen zouden genomen moeten worden wanneer een werknemer bij een organisatie weggaat?   **Zeker weten dat hij de geheimen van een organisatie niet doorverteld. Zorgen dat diegene ook geen toegang meer heeft tot de informatie.**  Personele security maatregelen  Personele security maatregelen zijn onder te verdelen in:   * Maatregelen voor indiensttreding, vooral gericht op de werving en selectie van nieuw personeel, zoals bijvoorbeeld:   • werving, selectie- en aannameprocedures;  • controleren cv en getuigschrift en referenties;  • antecedentenonderzoek;  • verklaring omtrent gedrag (VOG);  • geheimhoudingsverklaring;  • laten invullen van vragenlijst;  • procedure extern personeel/inhuur.   * Maatregelen bij in dienst zijn, zoals:   • security opleidingen/bewustzijn;  • gedragscode;  • functionerings- en beoordelingsgesprekken;  • beloning- en sanctiebeleid.   * Maatregelen bij vertrek, te weten:   • intrekken autorisaties;  • inleveren pasjes, sleutels, telefoon e.d.;  • checklist laatste dag;  • exitgesprek met leidinggevende;  • ontslag-op-staande-voet-procedure.  **Opdracht 4**   * In Nederland kent men op meerdere locaties datacenters. Datacenters worden fysiek beveiligd. Welke fysieke beveiligingen worden er toegepast bij datacenters?   **Terreinafcheiding, buitengevel, hang- en sluitwerk, zonescheiding en compartimentering, opbergmiddelen, indringerdetectiesystemen, CCTV, verlichting, toegangsverleningssysteem.**   * De irisscan is een biometrische beveiligingsmethode. Welke andere biometrische beveiligingsmethode wordt bij datacenters toegepast?   **Vingerscanner, gezichtsherkenning.**   * Waarom worden serverruimtes bij bedrijven niet op de begane grond geplaatst maar op de eerste verdieping?   **Als er een lek is heeft de serverruimte er geen last van. Beter beveiligd tegen inbraak.**  Fysieke security maatregelen (bouwkundige en elektronische)  Bouwkundige security maatregelen bestaan uit het vakkundig ontwerpen, bouwen en beheren van onder andere verstevigde muren, goedgekeurd hang- en sluitwerk op bereikbare ramen en deuren, het afschermen van glaspartijen en het afschermen van  ventilatieopeningen. Voorbeelden hiervan zijn:   * terreinafscheiding (hekwerken, grachten, barrières, poort); * buitengevel (steens metselwerk, beton, kunststof e.d.); * hang- en sluitwerk (SKG-normering); * zonescheiding en compartimentering; * opbergmiddelen (kluis, kasten e.d.); * indringerdetectiesysteem (radar, infrarood, geluid, combinatie); * closed circuit TV (CCTV); * verlichting (permanent, schrik, dag-nacht); * toegangsverleningssysteem (slagboom, tourniquet, kaartlezer, irisscan e.d.).   **Opdracht 5**  Computers bij bedrijven zoals workstations, laptops en servers worden beveiligd met verscheidende ICT-security maatregelen. Je eigen pc en/of laptop is uiteraard ook beveiligd. In deze opdracht ga je je eigen pc en/of laptop onderzoeken op ICT-security maatregelen.   * Is er een virusscanner op pc en/of laptop geïnstalleerd? En zo ja welke virusscanner gebruik je? Is deze virusscanner gratis of moet je hiervoor betalen?   **Ja, avast. gratis**   * Wat zijn de verschillen tussen een gratis antivirusscanner en een virusscanner waarvoor je moet betalen?   **Betaald is meestal beter en dan kan je hem beter naar eigen wensen aanpassen.**   * Op je pc en/of laptop maak je gebruik van computer accounts (gebruikersnaam en wachtwoord). Heb jij een wachtwoord ingesteld op he gebruikersnaam? Wat is de lengte (aantal karakters) van dit wachtwoord? Gebruik je ook hoofdletters, cijfers en bijzondere tekens in je wachtwoord?   **Ja, 9, ja**   * Is de firewall op je pc en/of laptop ingeschakeld? Zo ja en zo nee waarom niet?   **Ja het is veiliger**   * Maak je zelf regelmatig een backup van je pc en/of laptop? Zo nee waarom niet.   **Ja**   * Bij kerncentrales gebruikt men ook pc maar deze pc zijn niet aangesloten op het internet. Leg uit waarom men dit doet?   **Zo kan die niet vanuit het internet aangevallen worden om gegevens over kernenergie te stelen.**  ICT-security maatregelen  Voorbeelden van ICT-security maatregelen zijn:   * backupregeling; * virusscanners; * encryptie (versleuteling van informatie); * stand alone systeem (dus los van internet); * firewall(s); * ICT-authenticatie en autorisatie (wie ben je en wat mag je op het netwerk); * wachtwoordbeheer.   Voorkennis en te bestuderen:   * Bekend zijn met het zoeken op internet.   Hoe haal je een voldoende voor deze opdracht?   |  |  |  | | --- | --- | --- | | 1 | Zet alle antwoorden van de opdrachten in een Word-document. | ❑ | | 2 | Laat je antwoorden controleren door je docent. | ❑ | | 3 | Upload je gecontroleerde en gecorrigeerde Word-document in It´s Learning. | ❑ | |