

De rol van fysieke beveiliging in het Security Management proces.

U kan uw data nog zo goed elektronisch beschermen, zonder fysieke beveiliging is het allemaal vergeefse moeite. Want wat helpen firewalls en virusscanners indien onbevoegden zomaar uw serverzaal en kantoren kunnen binnenwandelen? Een efficiënt toegangscontrolesysteem kan u op dit gebied verder helpen.

Allereerst dient u ervoor te zorgen dat ongewenste individuen uw terrein niet kunnen binnendringen. Hiertoe kunt u zowel fysieke als elektronische beveiligingsmiddelen inzetten. Fysieke beveiligingsmiddelen zijn bijvoorbeeld inbraakwerende deuren en ramen, slagbomen en omheiningen. Ze vormen een eerste barrière voor potentiële inbrekers of vandalen en er gaat een preventieve werking van uit. Mocht iemand toch willen inbreken, dan werken ze echter uitsluitend vertragend; ze houden zelden iemand echt buiten de deur.

Vandaar dat u ze met elektronische hindernissen moet combineren. Toegangscontrolesystemen verhinderen dat niet-geautoriseerde personen een gebouw of ruimte betreden; sensors en camerabewaking detecteren inbreuken op de beveiliging en kunnen snel hulpdiensten (politie of bewakingsdienst) inschakelen.

Op het vlak van fysieke beveiliging valt er weinig nieuws te melden. Het aanbod is al jaren voldoende uitgebreid. Bovendien is het aanbod dermate geperfectioneerd dat nieuwe verbeteringen enkel nog details betreffen.

Echt grote veranderingen zijn er te zien bij de toegangscontrolesystemen. Hun traditionele toepassing is in de loop der jaren met talrijke functies uitgebreid. In plaats van enkel als vervanging van sleutels te dienen, bieden veel van deze systemen nu ook de mogelijkheid na te gaan wie zich waar in het gebouw bevindt. Dit is vooral bij calamiteiten, zoals een brand, zeer nuttig.

Tevens is de registratie van bezoekers een standaardprocedure geworden voor heel wat bedrijven. Op die manier kunnen er bezoekerslijsten worden gemaakt. Deze zorgen ervoor dat er bij problemen (zoals diefstal) kan worden nagegaan wie er op dat moment op de plaats van de misdaad was (traceerbaarheid).

Daarnaast wordt de badge tegenwoordig voor heel wat meer gebruikt dan alleen het openen van deuren. Zo worden ze toegepast om toegang tot parkeergarages te krijgen, de slagbomen van het terrein te openen, zich als pc-gebruiker aan te melden en zelfs om de lunch in de cafetaria te betalen.

Op deze manier wordt het steeds moeilijker voor een buitenstaander om ongemerkt in uw bedrijf rond te wandelen en van uw faciliteiten gebruik te maken.

Secure Connection kan u naast informatiebeveiliging ook adviseren op het gebied van fysieke beveiliging. Voor meer informatie kunt u contact met ons opnemen.

De Security Mirror - Deel III

Organisaties zijn in de loop der tijd steeds afhankelijker geworden van het communicatiemedium dat e-mail heet. Als het over e-mail gaat dan wordt ook direct gedacht aan ongewenste berichten (spam) die mogelijk virussen met zich meedragen. Niet alleen het beschermen tegen het binnendringen van dit soort berichten op uw netwerk is van belang maar ook het passeren ervan! Als uw instelling namelijk een eigen mailserver heeft dan kan het zijn dat deze server gebruikt wordt als open mail relay. Dit betekent dat uw mailserver e-mail doorstuurt naar adressen die lokaal (op uw netwerk) niet bekend zijn. In het kort gezegd betekent dit dat spammers ongemerkt uw mailserver kunnen misbruiken om ongewenste e-mailberichten te versturen.

Secure Connection biedt de mogelijkheid om een technische quickscan uit te voeren zodat u onder andere een beeld krijgt of uw instelling voldoende beschermd is tegen het binnendringen en/of passeren van de ongewenste e-mailberichten waardoor de beschikbaarheid van uw mailserver gewaarborgd kan worden.

Actueel

26 mei 2005

De 6 stappen om virussen en wormen te verwijderen!

Regelmatig verschijnen er berichten van mensen wiens PC geïnfecteerd is. De meesten willen hun data back-uppen of systeem stabiel krijgen voordat ze hun PC formatteren. Het Internet Storm Center heeft een artikel gepubliceerd waarin in zes stappen wordt uitgelegd hoe Windows XP malware verwijderd kan worden.

Stap 1

Schakel System Restore uit en zorg dat je de juiste tools, zoals anti-spyware en anti-virus, bij de hand hebt.

Stap 2

Start de computer op in Veilige Mode en draai Autoruns.

Stap 3

Draai msconfig.exe en zoek naar verdrachte processen en services.

Stap 4

Scan de computer met anti-virus en anti-spyware software.

Stap 5

Installeer en draai BHODemon.

Stap 6

Start de computer opnieuw op en kijk met TCPView en Process Explorer welke verdachte processen en verbindingen nog actief zijn.