Zorgen voor een goede beveiliging van je IT-omgeving: waar begin je?

Vaak spelen er in organisaties uitdagingen in de vorm van budget en gebrek aan kennis. Wanneer je niet weet wat de gevaren zijn – en dat zijn er tegenwoordig nogal wat – en je een beperkt budget ter beschikking hebt, zal de prioriteit nooit liggen bij de juiste security producten. Na een nieuwe bedreiging die aangehaald wordt tijdens het achtuurjournaal denk je wel: hebben wij het wel goed op orde?

Het nieuwe werken brengt ook uitdagingen met zich mee. Jouw medewerkers werken steeds vaker thuis met verschillende soorten devices. Hierdoor is bedrijfsdata opgeslagen op allerlei servers en (mobiele) apparaten. De coronacrisis legde in veel organisaties de zwakke plekken van hun security bloot. Waar je voorheen op netwerkniveau kon beveiligen moet je nu een virtuele beveiligingsmuur laten aanbrengen.

De gedachte dat je als organisatie dus grote stappen moet maken met security is meer aanwezig dan enkele jaren geleden. Toch krijgen dringende zaken die impact hebben op de bedrijfsvoering en de business vaak voorrang in de dagelijkse sleur. Een strategische aanpak op het gebied van security is daarom noodzakelijk. Je ontkomt er als organisatie niet aan om iemand aan te wijzen die zich kan bezighouden met het beveiligen van data, en daar dus ook tijd voor heeft.

IT-beheerder of alleskunner?

Bij de meeste bedrijven is de IT-beheerder tegenwoordig vaak IT-Manager, applicatiebeheerder én dataonderhouder. Hij heeft alle rollen op zich genomen en is een alleskunner geworden. Het is niet mogelijk om overal de beste in te zijn. Zonder budget om kennis in te kopen of om hulp in te schakelen zal je ‘veilige’ omgeving niet meer zo veilig zijn.

Waar in het verleden vaak firewalls werden gebouwd die organisaties zagen als ‘een grote kasteelmuur’ voor maximale controle, is dit nu niet meer haalbaar. Steeds meer applicaties zijn via de cloud te benaderen en jouw gebruikers kunnen via het internet overal toegang krijgen tot bedrijfsdata. Denk bijvoorbeeld aan tools zoals Dropbox. Hoe ga je die data in de cloud beschermen? Het redeneren wordt anders: je moet niet meer denken vanuit de kasteelmuren (firewalls) maar vanuit de verschillende soorten data. Daar kun je kleinere muurtjes omheen bouwen in elke applicatie die je gebruikt. Een vorm van versleuteling en data loss prevention technieken zorgen ervoor dat je op korte termijn stappen kunt zetten. Op de lange termijn heb je een strategie nodig. Wat is privacygevoelige data binnen jouw organisatie? Het is belangrijk om hier policies voor op te stellen.

Alert blijven

Alert blijven is de boodschap. Het is belangrijk om alle apparaten in jouw netwerk te monitoren. 100% zekerheid geeft het niet, maar je kunt zo wel zaken terughalen.

Meer informatie?

Heb je een vraag of wil je meer weten? We staan je graag te woord. Onze medewerkers zijn bereikbaar via telefoonnummer 0180-318888 of per mail: tebovisie@tebovisie.nl