
Telefonie, internet, betaalverkeer en beveiliging samen over een enkele breedbandverbinding - niet zonder risico!

Inleiding: Bedrijfscommunicatie verloopt meer dan ooit via telecom en internet. Daarvoor is een imposante infrastructuur neergelegd. Was twintig jaar geleden een overzichtelijk vlechtwerk van koperkabel nog voldoende voor gesproken woord en een telexboodschap. Tegenwoordig verwerken tienduizenden servers in futuristische datacentra 24/7 de meest complexe digitale informatie, gevoed uit razendsnelle glasvezelnetten. Met het resultaat daarvan zijn we kinderlijk vertrouwd. Geen winkel meer waar je niet kunt pinnen, geen bedrijf dat niet op afstand is beveiligd. Maar al die onmisbare telecomdiensten lopen uit kostenoverwegingen nogal eens over een enkele breedbandverbinding. En dat brengt risico's met zich mee. Het gaat immers om zeer uiteenlopende disciplines. Autonome diensten aangeboden door concurrerende leveranciers. Deze *providers* hebben vooral oog voor de kwaliteit van hun eigen toepassing en kunnen niet altijd overzien of hun dienstverlening andere spelers verdraagt die van dezelfde telecom-breedbandverbinding gebruik willen maken. Het is bijna onmogelijk om uit het enorme aanbod van diensten een verantwoorde keuze te maken. Anderzijds is duidelijk dat het een niet ten koste mag gaan van het ander. Het is van belang dat beide diensten (betalen en alarmeringen) goed blijven werken, ook al gebruiken ze dezelfde telecomlijn. Om te weten hoe een goede werking verkregen kan worden is deze checklist opgesteld.

Het meest belangrijke risico is dat verschillende leveranciers / installateurs / providers van diensten die allemaal gebruik maken van die enkele breedbandverbinding elkaar negatief kunnen beïnvloeden. Dat kan betekenen dat op een willekeurig moment een van die diensten niet meer werkt, met alle gevolgen van dien.

Een bijzonder aandachtspunt voor alle diensten via een breedbandverbinding is de beschikbaarheid van de verbinding bij een netspanningsuitval. Zowel de leverancier van inbraaksignalering als de leverancier van de betaalterminal kan hier het juiste advies en oplossing verzorgen.

Wat te doen?: Schakel een gespecialiseerd telecom-adviesbureau in. Uw branche-, MKB-, of Retail-organisatie kan daarbij behulpzaam zijn.

Voordat u uw telecommunicatie voorziening gaat (1) aanschaffen, (2) veranderen of (3) uitbreiden is het verstandig alvast enige basisgegevens te verzamelen. Deze gegevens zijn voorwaarde voor een gesprek met een leverancier voor aanpassingen, uitbreidingen, enz.

Deze publicatie is tot stand gekomen in samenwerking met de Betaalvereniging Nederland¹ en VEBON², de Vereniging van Beveiligingsondernemingen Nederland secties anti Inbraak-en Overval en Elektronisch Toegangsbeheer.

¹ Betaalvereniging Nederland, Gustav Mahlerplein 33-35 1082 MS Amsterdam

² VEBON Vereniging van Beveiligingsondernemingen Nederland, Boerhavelaan 40 2713 HX Zoetermeer – www.vebon.org

Situatie 1: *U begint een nieuw bedrijf of betreft een nieuw pand. U hebt nog geen telecommunicatie aansluiting op de locatie.*

Inventariseer en bedenk wat u wel en niet nodig hebt dan wel wilt:

Internet	Alleen email (zenden en ontvangen)? Of werkt u ook met een webwinkel?
Wi-Fi	Eigen gebruik? Of ook voor klanten, een hotspot?
Betaalautomaat / PIN	Een of meerdere? Mobiel of Vast?
Inbraak- en/of overvalalarm	Zijn er eisen van verzekeraar? Is er een collectief in de omgeving of is er sprake van een (bewaking)dienst die ondernemers samen inkopen?
Video bewaking op afstand	Wilt u opname van beelden of alleen "live" uitkijken? Wilt u politieondersteuning bij afwezigheid (avond en nacht)? Wilt u de inzet van een bewakingsdienst overdag? Wilt u de inzet van politie tijdens werkuren?
Overige wensen	Speciale eisen voor wat betreft de telecomaansluiting in combinatie met betaalautomaat / PIN? Kijk daarvoor hier op de website van de betaalvereniging ³

Informeer bij uw branchevereniging.

Vaak hebben zij al beproefde en uitgewerkte concepten specifiek voor uw branche. Sommige brancheverenigingen houden ook lijsten bij van betrouwbare leveranciers. Maak daar gebruik van.

Situatie 2: *U wilt inbraak- en overval-alarmdoormelding. U hebt al een contract voor de betaalautomaat/PIN en bijbehorende aansluiting. Waar moet u op letten?*

1. Zorg dat u beschikt over de contactgegevens van uw huidige telecomleverancier en dat u de contracten en voorwaarden bij de hand hebt, evenals het telefoonnummer van de helpdesk. Verzamel eenzelfde lijstje met gegevens van de leverancier van de betaalterminal.
2. Vraag de alarminstallateur naar de eisen gesteld aan de verbinding voor het doormelden naar uw alarmcentrale. Er is keuze uit de volgende typen: een enkelvoudige verbinding voor de lagere risico's en een meervoudige verbinding voor de hoge risico's. En ieder risico niveau heeft zijn eigen specifieke technische eisen aan de verbinding. Informeer naar de mogelijkheden!
3. Vraag de alarminstallateur of hij de leverancier van de betaalautomaat/PIN en/of de provider kent. En vraag hem of hij op de hoogte is van de technische struikelblokken die bestaan bij aansluiting op een router van derden.

³ Hier de volledige link: <http://www.betalvereniging.nl/kaartbetalingen/datacommunicatie/>

Situatie 3: *Uw alarmdoormelding verloopt via een ouderwetse telefoonlijn of is aangesloten via internet en u wilt ook een betaalautomaat/PIN. Waar let u op?*

1. Zorg dat u de contactgegevens van uw huidige leveranciers zoals het beveiligingsbedrijf en uw telecomleverancier beschikbaar hebt, evenals het telefoonnummer van hun servicedienst.
2. Zijn er bijzondere eisen voor de alarmdoormelding via breedband? Uw beveiligingsbedrijf zal aangeven hoe de beide diensten optimaal via breedband kunnen worden gerealiseerd.
3. Vraag de leverancier van de pinbetaaldienst naar zijn eisen op telecommunicatiegebied om continue beschikbaarheid voor uw klanten te kunnen garanderen. En heeft de leverancier van de pinbetaaldienst ook een aanbod op het gebied van alarmering? In veel gevallen zal de leverancier van de pinbetaaldienst (een bank of een betaaldienstleverancier) u doorverwijzen naar de betaalautomaatleverancier, die de technische eisen beter kent.

Tot slot

- Vergeet na de migratie naar breedbanddiensten niet om (ongebruikte) telefoonlijnen op te zeggen. Dit scheelt u kosten!
- De alarmdoormelding werkt niet (of is niet betrouwbaar) als die wordt aangesloten op de telefoonaansluiting van een router. Die aansluiting is bedoeld voor spraak over internet. Vakterm: Voice over IP ofwel VoIP.

Voor het vinden van erkende beveiligingsbedrijven met kennis van zaken zie [deze](#) link naar de informatiesite van het CCV⁴, Preventiecertificaat.nl⁵.

⁴ Het CCV; het Centrum voor Criminaliteitspreventie en Veiligheid in Utrecht

⁵ Hier de volledige link; <http://www.preventiecertificaat.nl/>