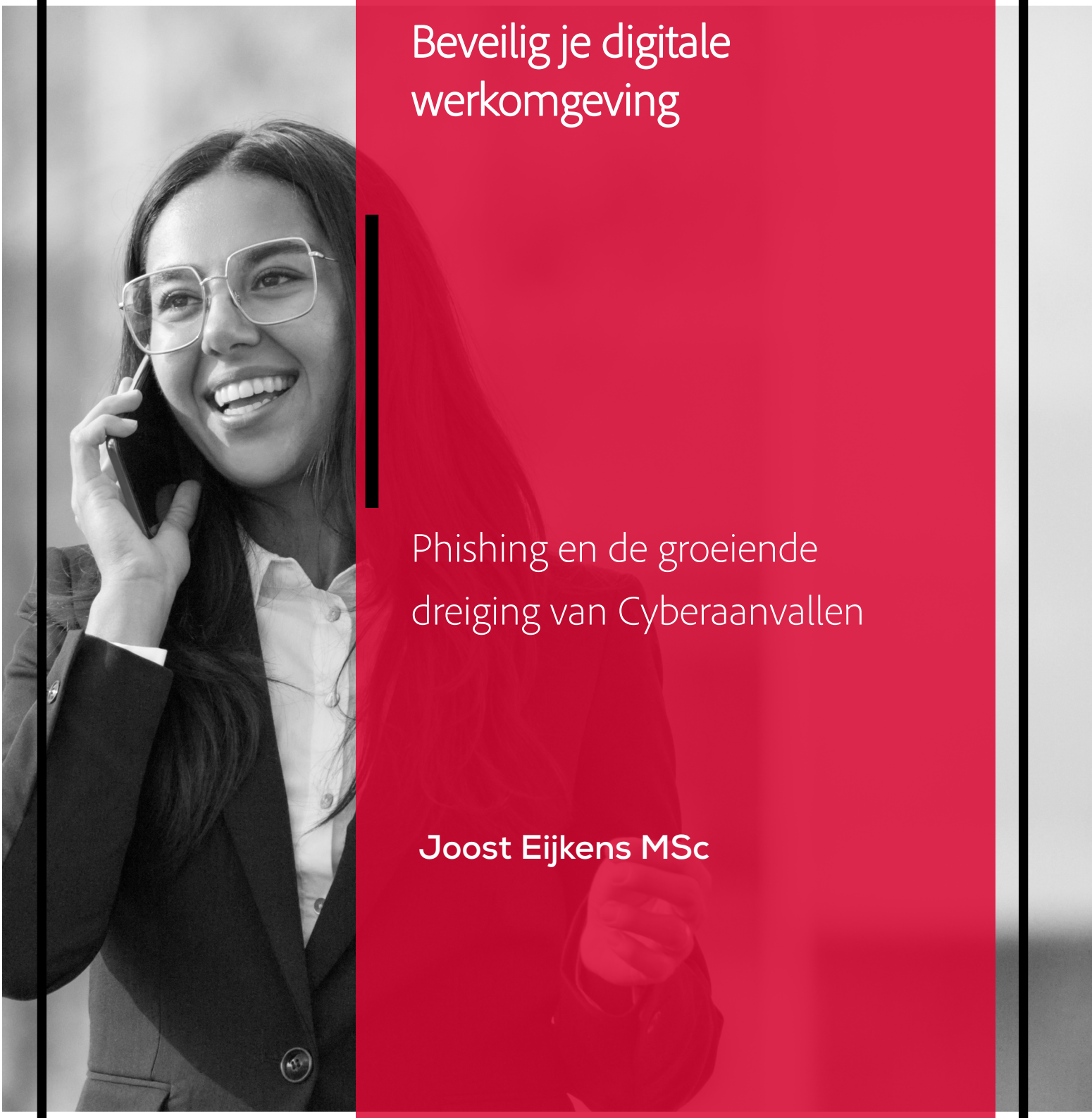


Beveilig je digitale werkomgeving

Phishing en de groeiende dreiging van Cyberaanvallen

Joost Eijkens MSc

Inleiding

2024 wordt een belangrijk jaar voor cybersecurity. Een nieuwe wet is in de maak en die verplicht duizenden organisaties om maatregelen te nemen tegen digitale aanvallen. Wat gaat de nieuwe wetgeving beteken voor bedrijven?

Phishing en de groeiende dreiging

Wat gaat de nieuwe wetgeving betekenen voor bedrijven?
Met de wet NIS2, wordt de controle en naleving op het gebied van digitale veiligheid vanaf oktober 2024 strikter. Volgens cybersecurity-expert Dave Maasland zou het wel eens om de grootste cybersecurity-wetgeving ooit kunnen gaan. Cyberaanvallen en de impact ervan nemen steeds verder toe. Als je kijkt naar wat er gebeurt in de wereld, heeft dat z'n weerslag op de digitale wereld. Denk aan wat we zien gebeuren tussen Israël en Hamas, maar ook de aanvallen tussen Rusland en Oekraïne. In beide oorlogen worden digitale aanvallen ingezet.

Het phishing' assessment van Cybersquare

Cybersquare een onderdeel van de Cardan Groep heeft het afgelopen jaar zich voorbereid op een phishing assessment waardoor we bedrijven en haar medewerkers bewust kunnen maken over de gevolgen van phishing. We bootsen een omgeving na waarin we op een eenvoudige manier het gevaar van cyberaanvallen in beeld brengen. Het gaat daarbij vooral over het herkennen van aanvallen en het vormen van beleid rondom email policy. Met haar phishing assessement gaat Cybersquare een stapje verder waar andere voorzieningen stoppen. De cyberspecialisten van Cybersquare ondersteunen bedrijven bij de te nemen preventieve maatregelen

We brengen zeer nauwkeurig in beeld waar de uitdagingen zitten voor bedrijven om zoveel mogelijk acties op te kunnen zetten om te voorkomen dat kwaadwillende infiltreren in bestaande systemen.

Graag neem ik jullie mee in de wereld van cybersecurity en specifiek in de diensten die wij als organisatie aanbieden om bedrijven bewust te maken van het gevaar van Fishing.

Waarom cybersquare ?

Cybersquare is sinds 2020 actief in Nederland. We hebben ons de afgelopen jaren verdiept in de wereld van Cybersecurity. We zijn de wereld rondgereisd om ons te verdiepen in de razendsnelle ontwikkelingen rondom digitale veiligheid. Zusteronderneming Technobility heeft zich ontwikkeld tot een volwaardig digitaal toegankelijkheidsbedrijf. Cybersquare biedt daar een extra

dimensie bij aan die ook de veiligheid van digitale werkomgevingen garandeert. Ik ben er trots op om deze mooie stap met de buitenwereld te kunnen delen. Ik neem jullie in deze eerste whitepaper mee in onze ambities en dienstverlening en hoop snel om met jullie in contact te komen om meer te vertellen over het belang van een digitaal veilige werkomgeving

Wie is Cybersquare?

Cybersquare is een wereldwijd georganiseerde security agency die klanten bedient vanuit kantoren in Nederland (Amsterdam en Tilburg)

Ons (development) team bestaat uit consultants die zelf afkomstig zijn uit de wereld van cybersecurity. Klanten hebben dus altijd contact met een consultant met een uitgebreid netwerk en ruime branche-ervaring. Onze cultuur is gebaseerd op de principes van verbondenheid, collegialiteit, samenwerking en uitdaging. Het is voor ons iedere dag een uitdaging om beter te presteren dan onze branchegenoten. Met minder zijn wij niet tevreden.

Slimme systemen

In een snel veranderende wereld zijn de waarden en normen uit het verleden niet langer meer de standaard voor de toekomst. Traditionele instrumenten moeten het afleggen tegen nieuwe, slimmere systemen en technologieën. Cybersquare conncentreert zich op preventieve maatregelen om gevaar van buitenaf tot een absoluut minimum te beperken om zodoende onheil van buitenaf te voorkomen.

Wij maken gebruik van ineigen huis ontwikkelde technologien en assessments met de diepgaande kennis van de huidige cybersecurity markt om de juiste instrumenten te ontwikkelen. Wij doen dat vanuit onze kennis en ervaring.

:

Cybersquare is op dit moment op zoek naar Partners met ambitie. Als partner wordt je meegenomen in een breed netwerk en maak je gebruik van het in eigen beheer ontwikkelde software programma.

Joost Eijkens (1961)

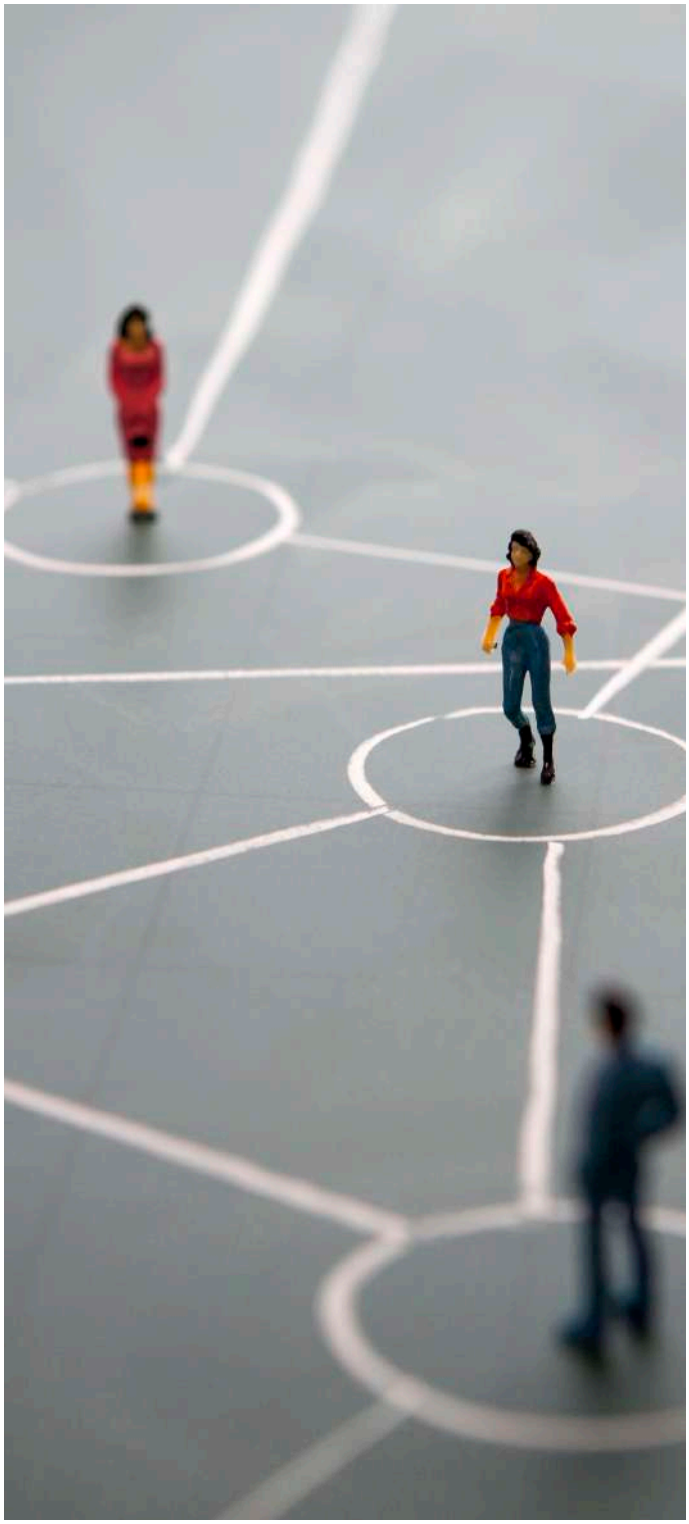
Eijkens heeft diverse organisaties en bedrijven ondersteund en aan de basis gestaan van diverse start- als scale ups en daarmee zijn bijdrage geleverd aan grootschalige technologische producties en ontwikkelingen. Zijn ervaring als ondernemer met een groot (inter) nationaal netwerk, heeft erin geresulteerd dat Cybersquare in een relatief korte periode een enorm netwerk aan klanten heeft geactiveerd. Het in eigen beheer ontwikkelt 'phishing' Assessment draagt bij aan een effectieve manier waardoor bedrijven en organisaties snel in staat worden gesteld om hun digitale wekomgeving op te beveiligingen en op orde te brengen.

I : www.cybersquare.nl
E : info@cybersquare.nl
P: +31 88 5004090
M:+ 31 6 51992021

- 96% van de Assessments draagt bij aan de optimale bewustwording van Cybersecurity dreigingen binnen bedrijven.

Wat is Phishing ?

Phishing is cyberaanval waarbij hackers proberen gevoelige informatie te verkrijgen, zoals wachtwoorden, bankgegevens en persoonlijke identificatiegegevens, door zich voor te doen als een betrouwbare bron via onderscheppingstechnieken zoals valse e-mails, websites en berichten. Phishing-vormen kunnen ook andere vormen aannemen, zoals smishing (phishing via sms), vishing (phishing via telefoon) en pharming (waarbij vervalste websites worden gebruikt om informatie te stelen).



1 Dreiging

De dreiging van phishing groeit gestaag, omdat cybercriminelen steeds geavanceerdere methoden ontwikkelen om gebruikers te misleiden en hun persoonlijke gegevens te stelen. Ze maken gebruik van social engineering om het vertrouwen van hun slachtoffers te winnen en hen te verleiden tot het delen van vertrouwelijke informatie. Phishing-aanvallen kunnen grote financiële schade veroorzaken en negatieve gevolgen hebben voor zowel individuen als organisaties

2 Aanvallen

Phishing is een vorm van cybercriminaliteit waarbij oplichters zich voordoen als een betrouwbare entiteit, zoals een bank, overheidsinstantie of bekend bedrijf, om persoonlijke gegevens te bemachtigen. Ze proberen gebruikers te misleiden door valse e-mails, sms-berichten of telefoontjes te sturen en hen te vragen om vertrouwelijke informatie te verstrekken, zoals inloggegevens, creditcardnummers of persoonlijke identificatiegegevens.

3 Voorkomen

Om phishing te voorkomen, is het belangrijk om altijd waakzaam te zijn en voorzorgsmaatregelen te nemen, zoals het controleren van de afzender van een e-mail, het vermijden van het klikken op verdachte links of het verstrekken van persoonlijke informatie via ongevraagde communicatiekanalen.

4 Het belang van phishing assessments

Regelmatige assessments zijn essentieel in zowel individuele als organisatorische contexten om de huidige situatie, prestaties en mogelijke risico's te evalueren. Ze helpen bij het identificeren van sterke punten, zwakke punten en gebieden die verbeterd kunnen worden.

5 Indentificatie

Assessments helpen bij het identificeren van zwakke punten, inefficiënties of knelpunten in processen, vaardigheden of systemen. Dit biedt inzicht in gebieden die verbeterd kunnen worden en stelt organisaties in staat om gerichte maatregelen te nemen.
Door periodieke assessments kunnen potentiële risico's en bedreigingen worden geïdentificeerd. Dit stelt organisaties in staat om passende maatregelen te nemen ter vermindering of voorkoming van deze risico's. Kortom, regelmatige assessments spelen een cruciale rol bij het identificeren van kansen, het verminderen van risico's, het verbeteren van prestaties en het nemen van geïnformeerde beslissingen.

6 Risico's en impact

Phishing is een vorm van cyberaanval die grote risico's met zich meebrengt en een aanzienlijke impact kan hebben. Hier zijn enkele belangrijke risico's en impactpunten:

- Identiteitsdiefstal
- Financieel verlies
- Schade aan reputatie
- Aantasting van gegevensbeveiliging
- Verlies van productiviteit

Het is belangrijk om bewust te zijn van de risico's en impact van phishing en om proactieve maatregelen te nemen om uzelf en uw organisatie te beschermen. Door regelmatig te oefenen met het herkennen van phishing-aanvallen en door beveiligingsmaatregelen te implementeren, kunt u de kans verkleinen dat u slachtoffer wordt van deze vorm van cybercriminaliteit.

Uitgelicht: Het Belang van phishing assessments

Phishing assessments zijn belangrijk omdat ze organisaties helpen om de veiligheid van hun informatie te waarborgen. Met een phishing assessment wordt getest hoe gevoelig de medewerkers van een bedrijf zijn voor phishing, oftewel het oplichten van mensen door middel van bijvoorbeeld valse e-mails die hen naar een nepwebsite leiden.
Een phishing assessment geeft inzicht in hoe goed medewerkers de gevaren van phishing begrijpen en hoe ze omgaan met verdachte e-mails. Het helpt organisaties om zwakke plekken te identificeren en eventuele tekortkomingen op het gebied van beveiliging aan te pakken.
Op basis van de resultaten van een phishing assessment kunnen organisaties gerichte trainingen en communicatiemiddelen ontwikkelen om medewerkers te helpen phishingaanvallen te herkennen en te vermijden. Dit helpt uiteindelijk om de veiligheid van de organisatie te verbeteren en te waarborgen.

Hoe assessments kunnen bijdragen aan de bewustwording

Assessments kunnen bijdragen aan bewustwording door medewerkers te laten zien hoe kwetsbaar ze zijn voor bedreigingen en risico's op de werkvloer. Door een verzameling van scenario's uit te voeren waarbij de medewerkers worden benaderd met (nep-) phishing e-mails of berichten, kunnen zij leren hoe ze deze verdachte situaties kunnen herkennen en vermijden.
Door het simuleren van deze situaties ervaren zij direct de consequenties van het onzorgvuldig omgaan met gegevens en het niet goed doorhebben van bedreigingen. Het kan ook leiden tot verhoogde veiligheidsmaatregelen en best practices binnen het bedrijf.
De resultaten van de assessments kunnen worden gebruikt om gerichte trainingen en workshops voor medewerkers te ontwikkelen. Vaak zijn deze niet alleen nuttig om medewerkers te leren hoe ze de organisatie beter kunnen beschermen tegen bedreigingen, maar ook om hen het belang van een veiligheidsbewuste cultuur binnen het bedrijf te laten begrijpen. Op deze manier kan een assessment bijdragen aan de bewustwording van medewerkers over de risico's en gevaren binnen hun organisatie en hen aanmoedigen om hun veiligheidsmaatregelen te verbeteren en te versterken

Over Cybersquare

CyberSquare is een branche specialist specifiek gericht op Phishing assessments. Computerbeveiliging, cyberbeveiliging of informatietechnologiebeveiliging (IT-beveiliging) is de core business van dit diefstal van of schade aan hun hardware, software of elektronische gegevens, alsmede tegen de verstoring of verkeerde aansturing van de diensten die zij leveren.

Het vakgebied wordt steeds belangrijker door de toegenomen afhankelijkheid van computersystemen, het internet en draadloze netwerkstandaarden zoals Bluetooth en Wi-Fi, en door de groei van "slimme" apparaten, waaronder smartphones, televisies, en de verschillende apparaten die het "internet der dingen" vormen. Vanwege de complexiteit, zowel in termen van politiek als technologie, is cyberbeveiliging ook een van de grootste uitdagingen in de hedendaagse wereld.

De kennis rondom cyber security is fragmentarisch en specifiek te noemen. De potentiële impact van cyberaanvallen en verstoringen neemt toe door verdergaande digitalisering De belangen zijn de afgelopen periode weer substantieel toegenomen. Het gebruik en daarmee de afhankelijkheid van ICT nemen nog altijd toe. ICT is een drijvende kracht achter onze maatschappij en steeds meer processen zijn hiervan volledig afhankelijk. Dreigingen blijven onverminderd hoog, en ook de zichtbaarheid van hulpmiddelen van statelijke actoren en cybercriminelen is gegroeid. De maatregelen houden geen gelijke tred met de belangen en kwetsbaarheden. Omdat de belangen substantieel toenemen, stijgt automatisch ook de potentiële impact van cyberaanvallen. Deze groeiende impact wordt onderstreept door de verstoringen die vorig voorjaar optraden door DDoS-aanvallen op Nederlandse banken en overheidsdiensten zoals DigiD. De grote afhankelijkheid van ICT voor onze maatschappelijke en persoonlijke veiligheid betekent dat een cyberverstoring of cyberaanval (in potentie) grote impact heeft op zowel de maatschappelijke als de persoonlijke veiligheid. Gebrek aan ICT duurzaamheid en toenemende koppeling vormen risico voor maatschappelijke veiligheid De ontwikkeling dat steeds meer apparatuur (waaronder medische apparatuur, voertuigen, televisies en huishoudelijke apparaten) aan internet verbonden is, zal doorzetten.

CyberSquare streeft naar uiterst realistische scenario's en maakt iedere phishing assessment geheel op maat. Dit stelt organisaties in staat om te oefenen met simulaties van de meest geraffineerde phishing-aanvallen, waardoor jouw team optimaal wordt voorbereid op een van de meest gebruikte manieren waarop hackers initiële toegang verkrijgen

Heb je nog vragen over het Phishing Assessment van Cybersquare of wil jij je meteen een afspraak inplannen ?
Neem dan nu contact op met Joost Eijkens, +31 88 500 40 90 of stuur een mail naar info@cybersquare.nl

Meer weten over Cybersquare, bezoek onze website www.cybersquare.nl