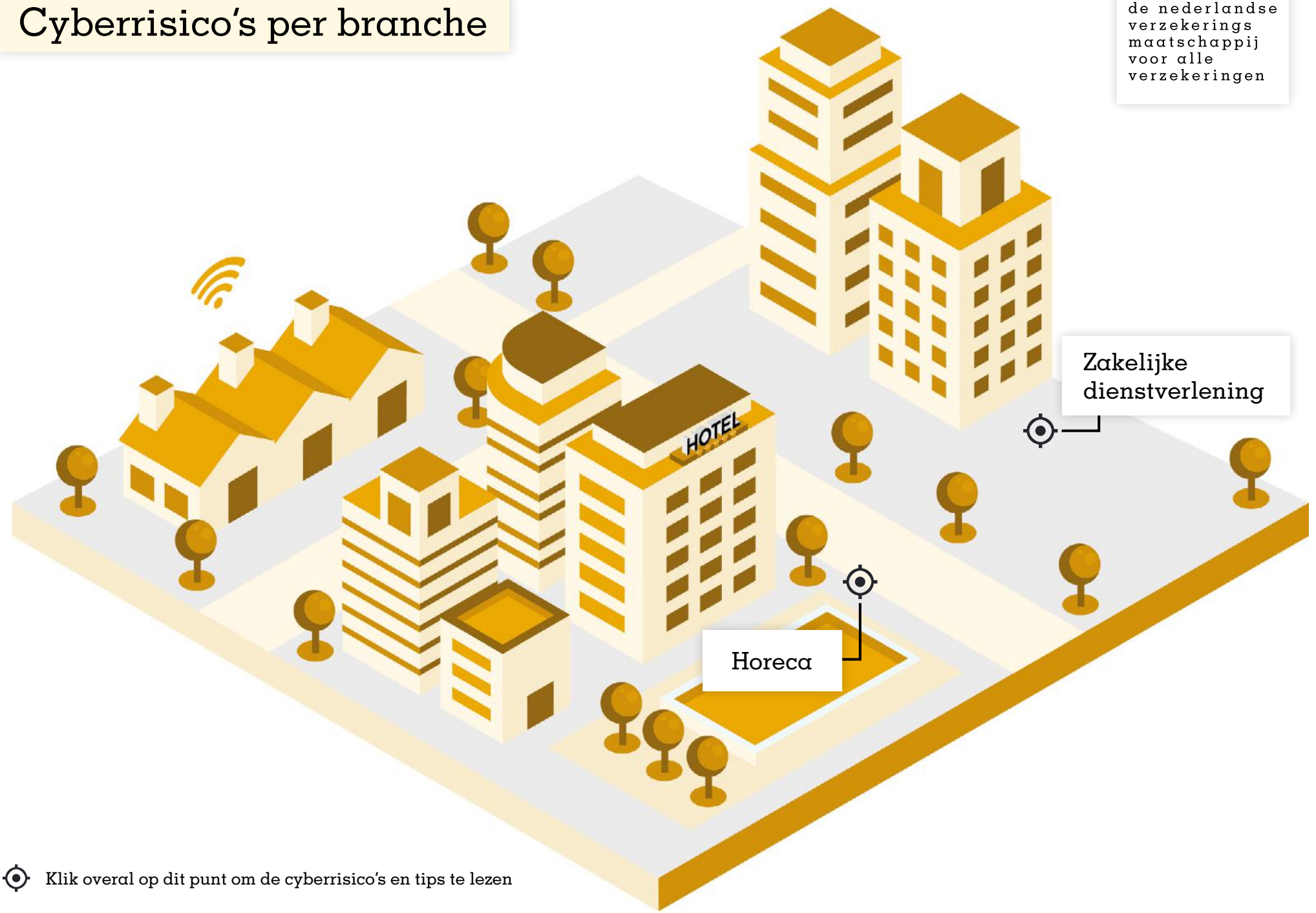
Cyberrisico's per branche

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

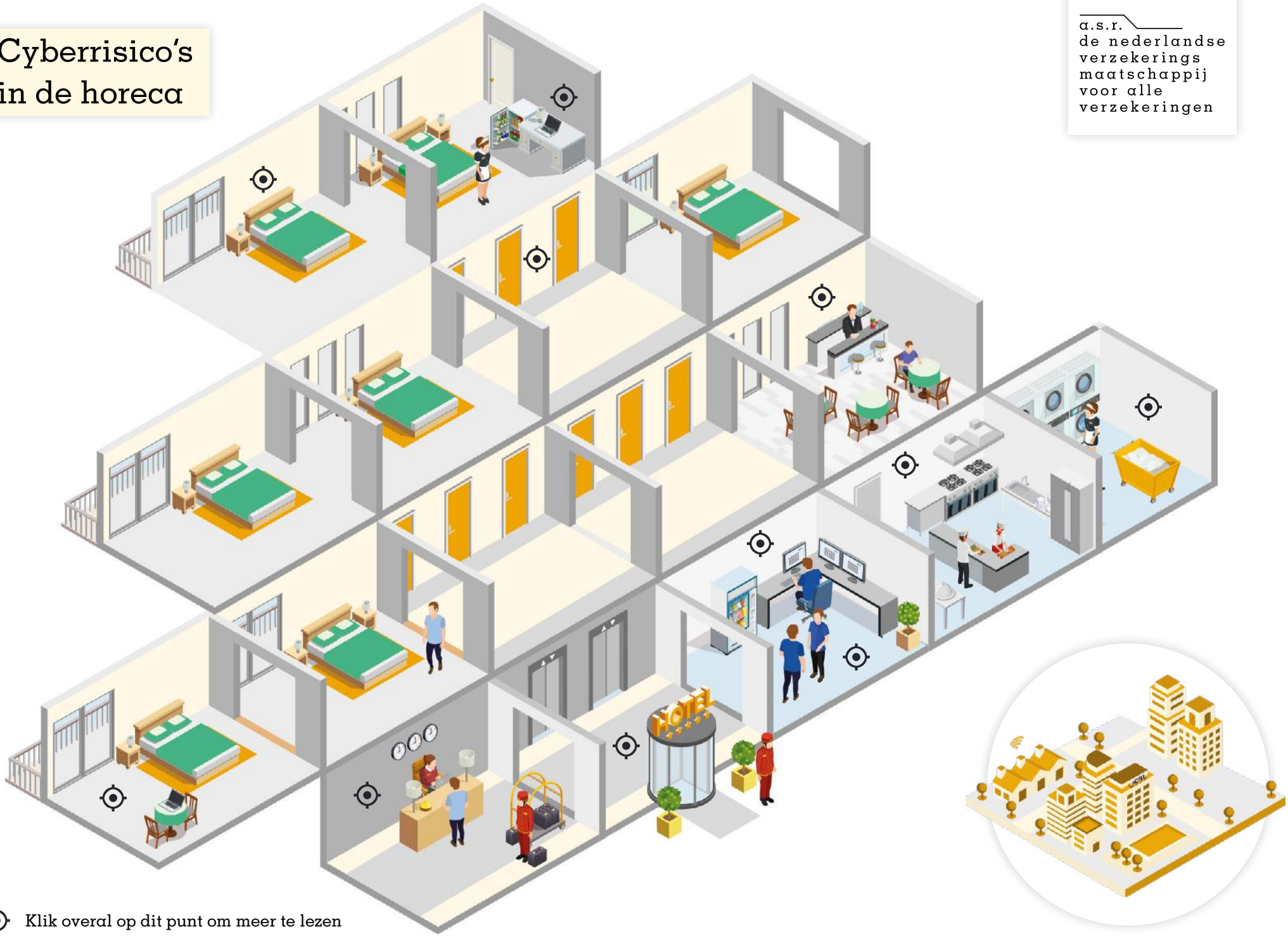


Klik overal op dit punt om de cyberrisico's en tips te lezen

39875_0919

Cyberrisico's in de horeca

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen



Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

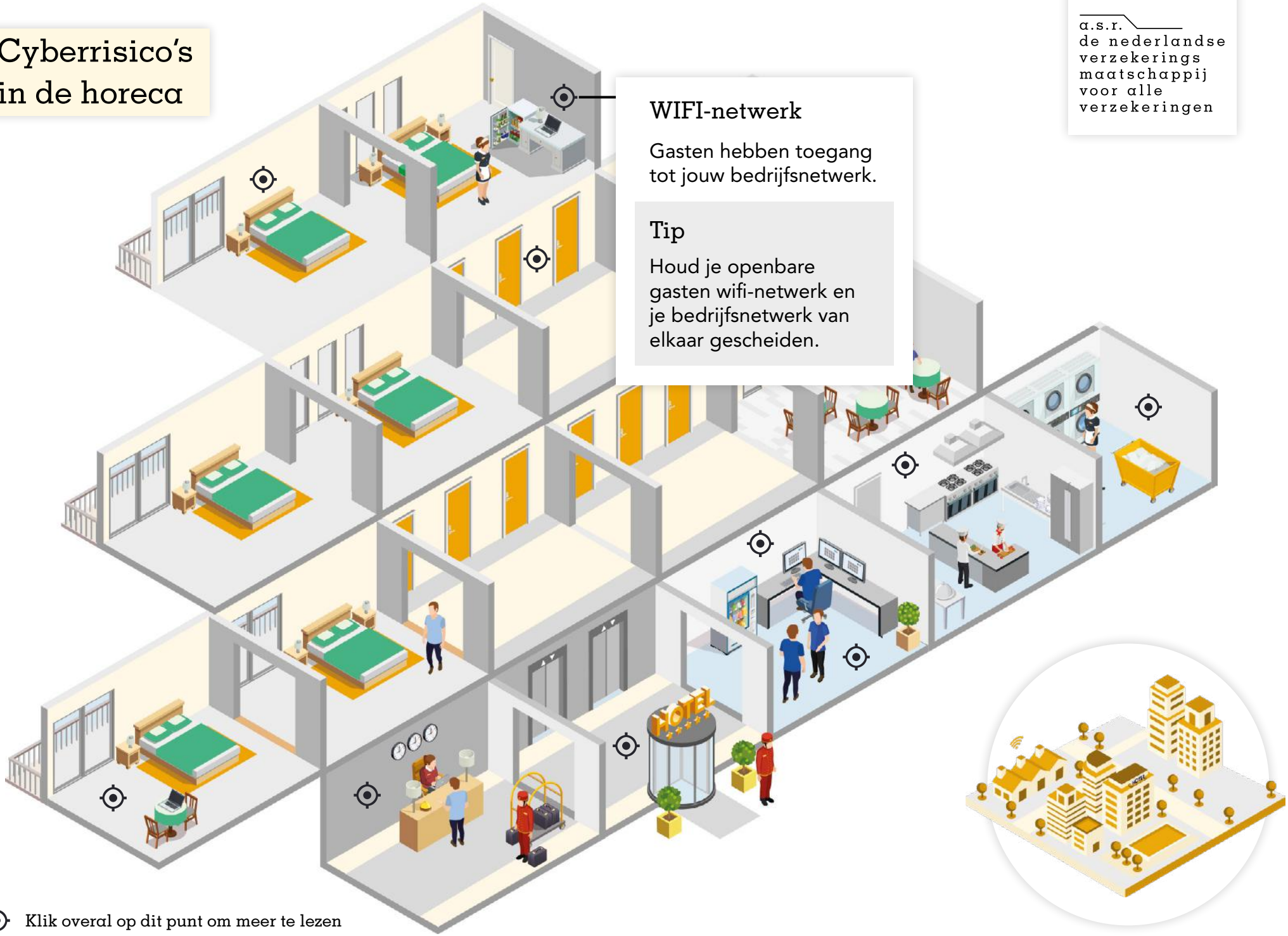
a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

WIFI-netwerk

Gasten hebben toegang tot jouw bedrijfsnetwerk.

Tip

Houd je openbare gasten wifi-netwerk en je bedrijfsnetwerk van elkaar gescheiden.



Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

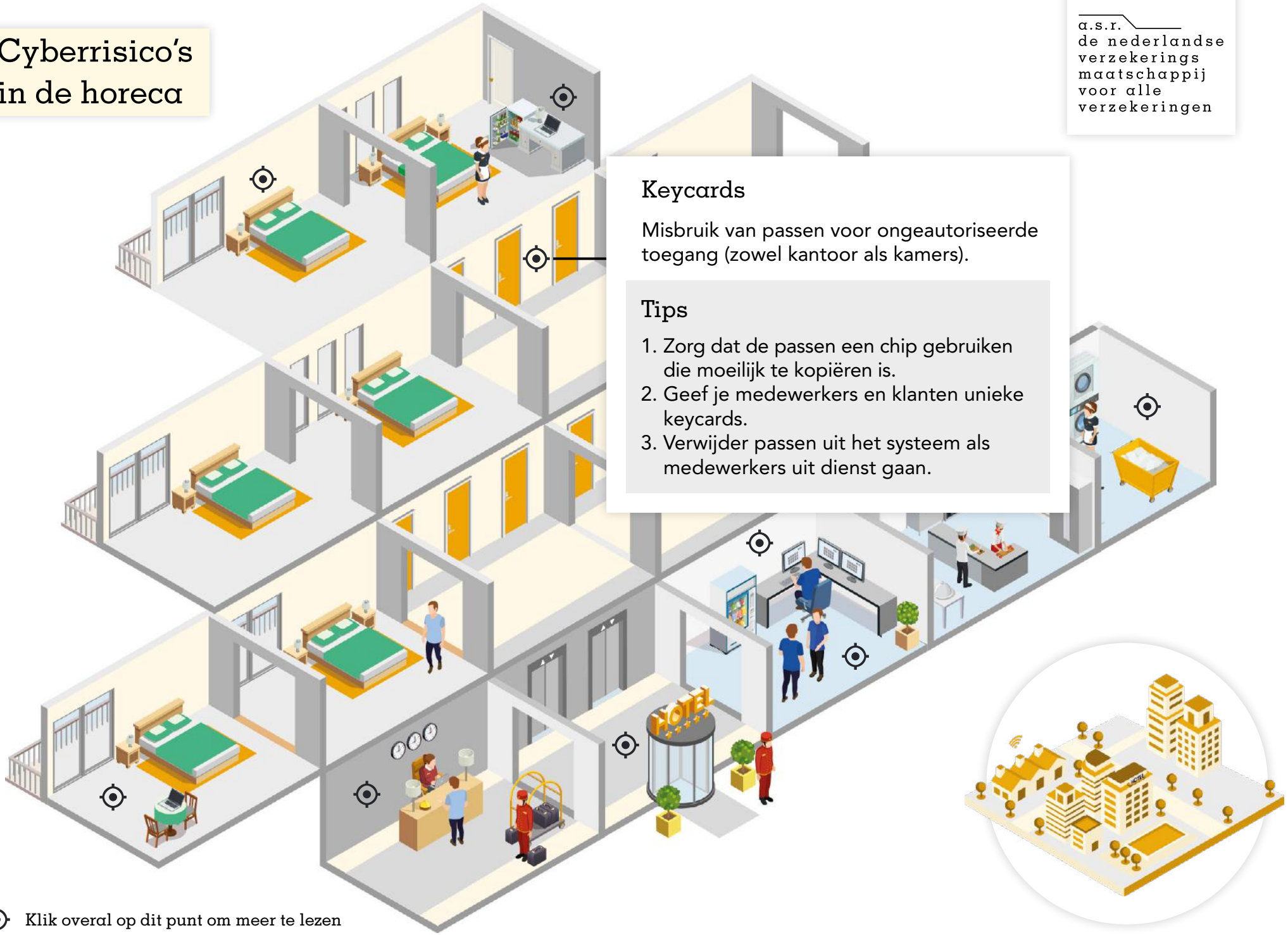
a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Keycards

Misbruik van passen voor ongeautoriseerde toegang (zowel kantoor als kamers).

Tips

1. Zorg dat de passen een chip gebruiken die moeilijk te kopiëren is.
2. Geef je medewerkers en klanten unieke keycards.
3. Verwijder passen uit het systeem als medewerkers uit dienst gaan.



Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

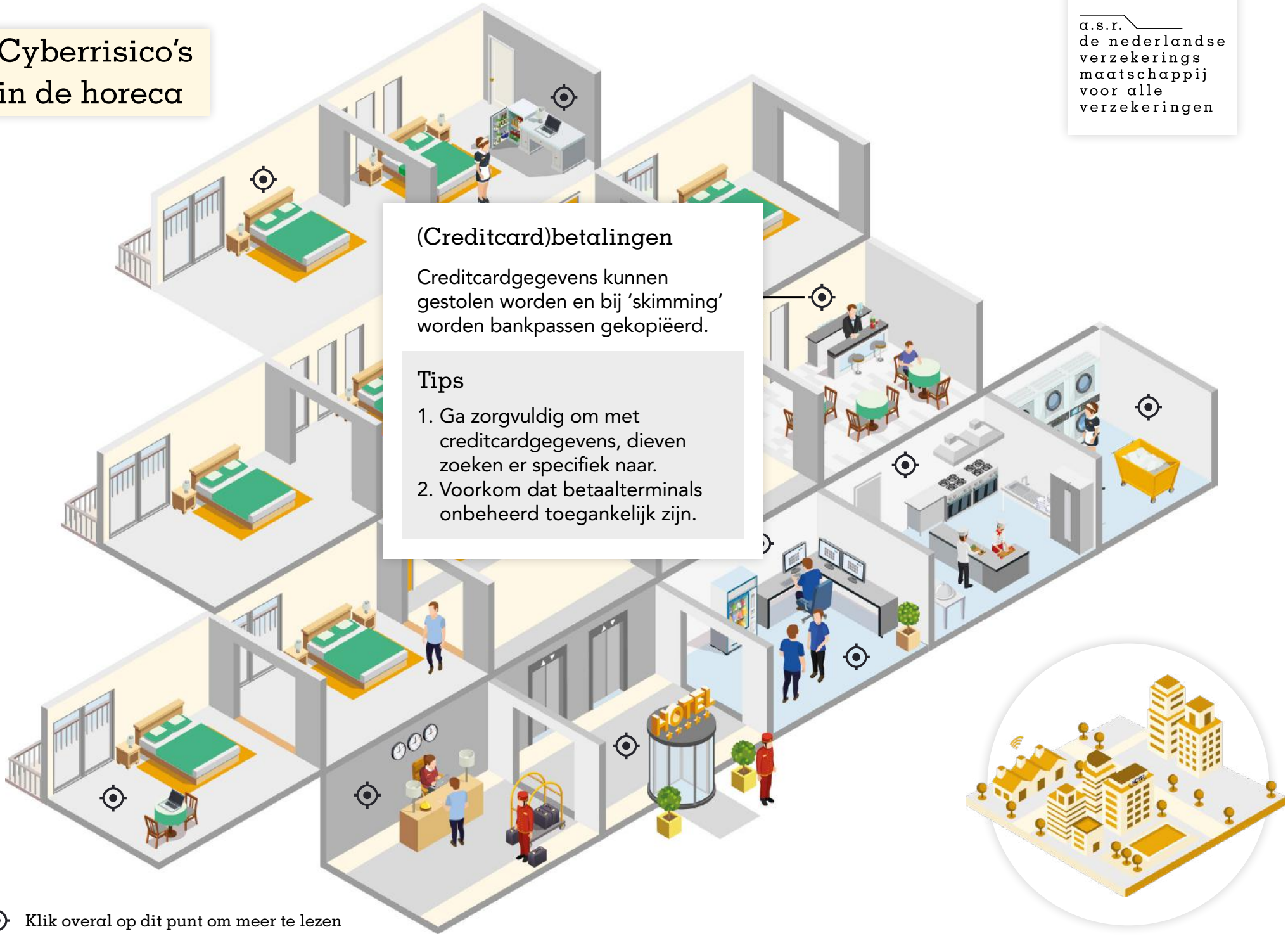
a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

(Creditcard)betalingen

Creditcardgegevens kunnen gestolen worden en bij 'skimming' worden bankpassen gekopiëerd.

Tips

1. Ga zorgvuldig om met creditcardgegevens, dieven zoeken er specifiek naar.
2. Voorkom dat betaalterminals onbeheerd toegankelijk zijn.



Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

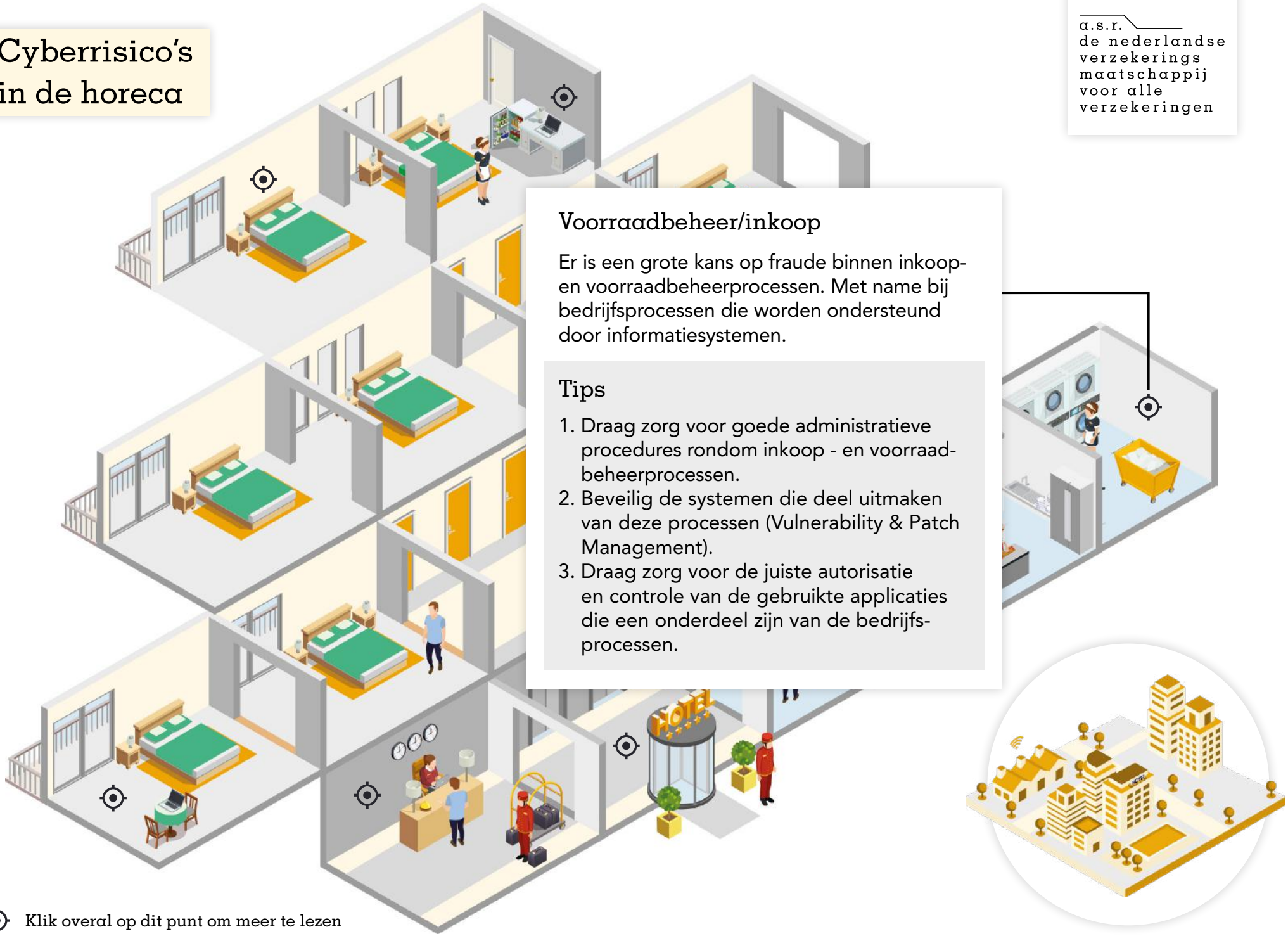
a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Voorraadbeheer/inkoop

Er is een grote kans op fraude binnen inkoop- en voorraadbeheerprocessen. Met name bij bedrijfsprocessen die worden ondersteund door informatiesystemen.

Tips

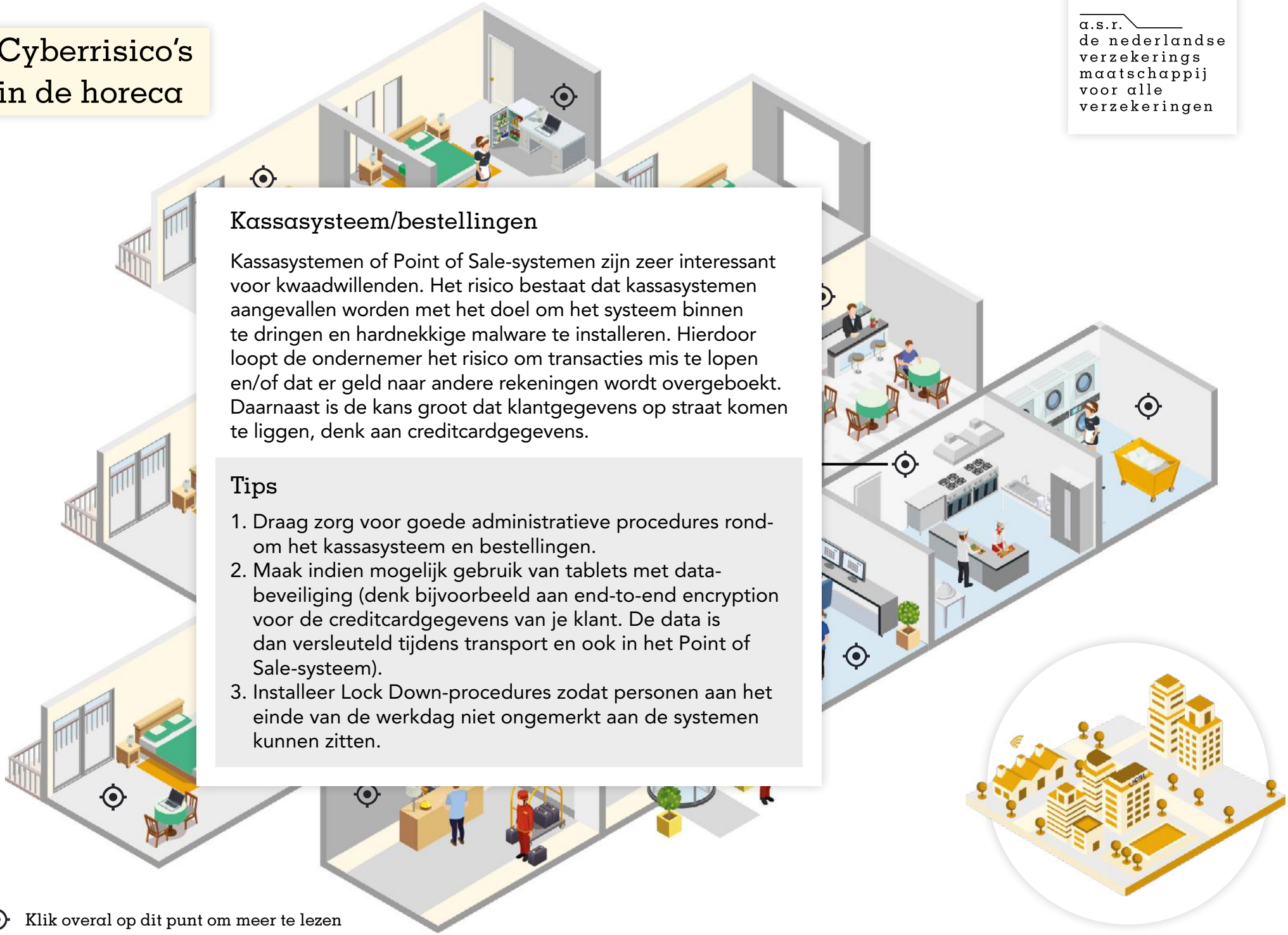
1. Draag zorg voor goede administratieve procedures rondom inkoop - en voorraad-beheerprocessen.
2. Beveilig de systemen die deel uitmaken van deze processen (Vulnerability & Patch Management).
3. Draag zorg voor de juiste autorisatie en controle van de gebruikte applicaties die een onderdeel zijn van de bedrijfs-processen.



Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen



Kassasysteem/bestellingen

Kassasystemen of Point of Sale-systemen zijn zeer interessant voor kwaadwillenden. Het risico bestaat dat kassasystemen aangevallen worden met het doel om het systeem binnen te dringen en hardnekkige malware te installeren. Hierdoor loopt de ondernemer het risico om transacties mis te lopen en/of dat er geld naar andere rekeningen wordt overgeboekt. Daarnaast is de kans groot dat klantgegevens op straat komen te liggen, denk aan creditcardgegevens.

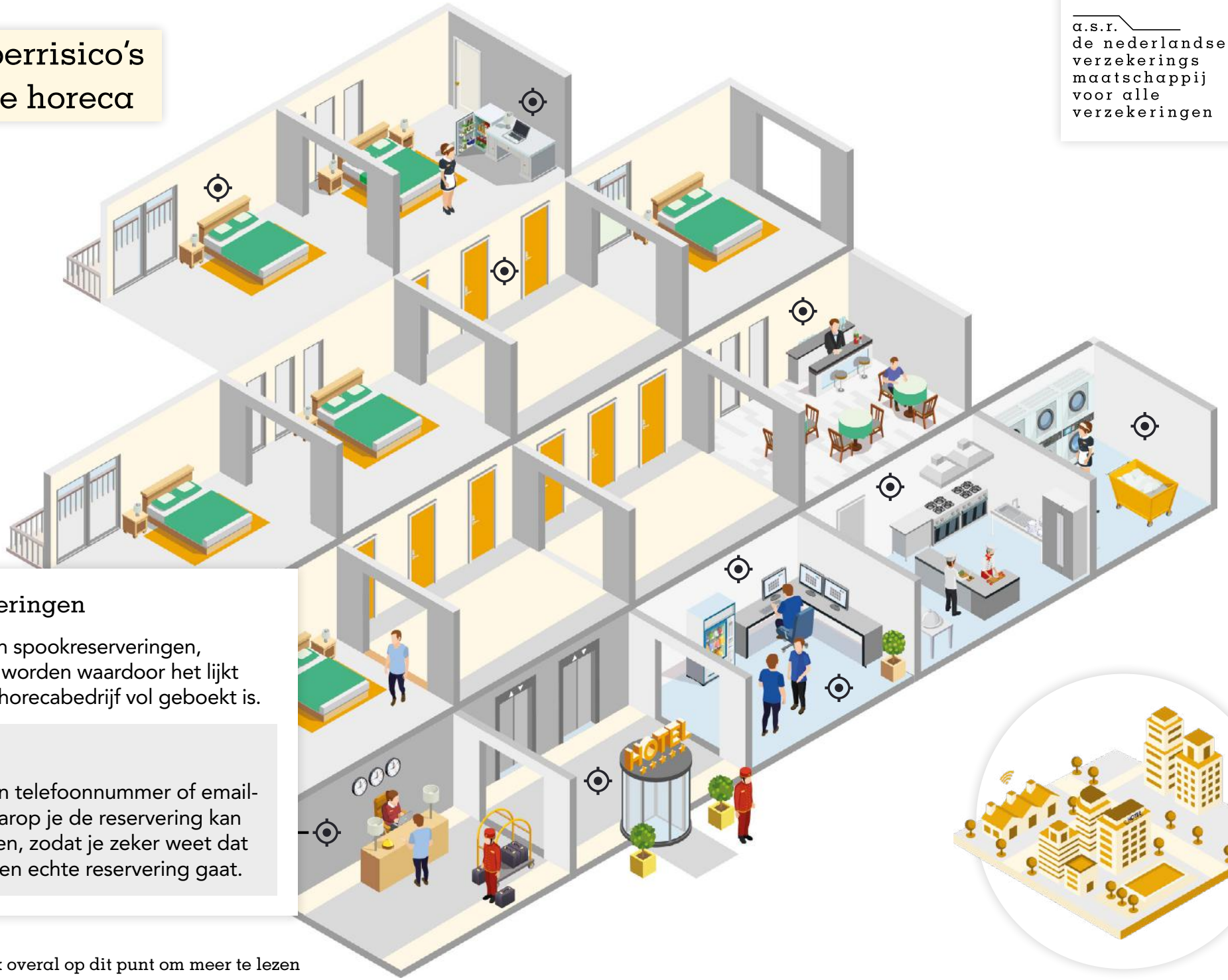
Tips

1. Draag zorg voor goede administratieve procedures rondom het kassasysteem en bestellingen.
2. Maak indien mogelijk gebruik van tablets met databeveiliging (denk bijvoorbeeld aan end-to-end encryption voor de creditcardgegevens van je klant. De data is dan versleuteld tijdens transport en ook in het Point of Sale-systeem).
3. Installeer Lock Down-procedures zodat personen aan het einde van de werkdag niet ongemerkt aan de systemen kunnen zitten.

Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen



Reserveringen

Er kunnen spookreserveringen, gemaakt worden waardoor het lijkt alsof jou horecabedrijf vol geboekt is.

Tip

Vraag een telefoonnummer of email-adres waarop je de reservering kan bevestigen, zodat je zeker weet dat het om een echte reservering gaat.

Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Camerabeveiliging

Camera's kunnen door buiten-staanders misbruikt worden om mee te kijken.

Tip

1. Zorg dat je camera's alleen via het interne netwerk of een VPN-verbinding te benaderen zijn.
2. Zorg dat elke camera een eigen wachtwoord heeft.
3. Werk regelmatig de software van de camera's bij.

Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

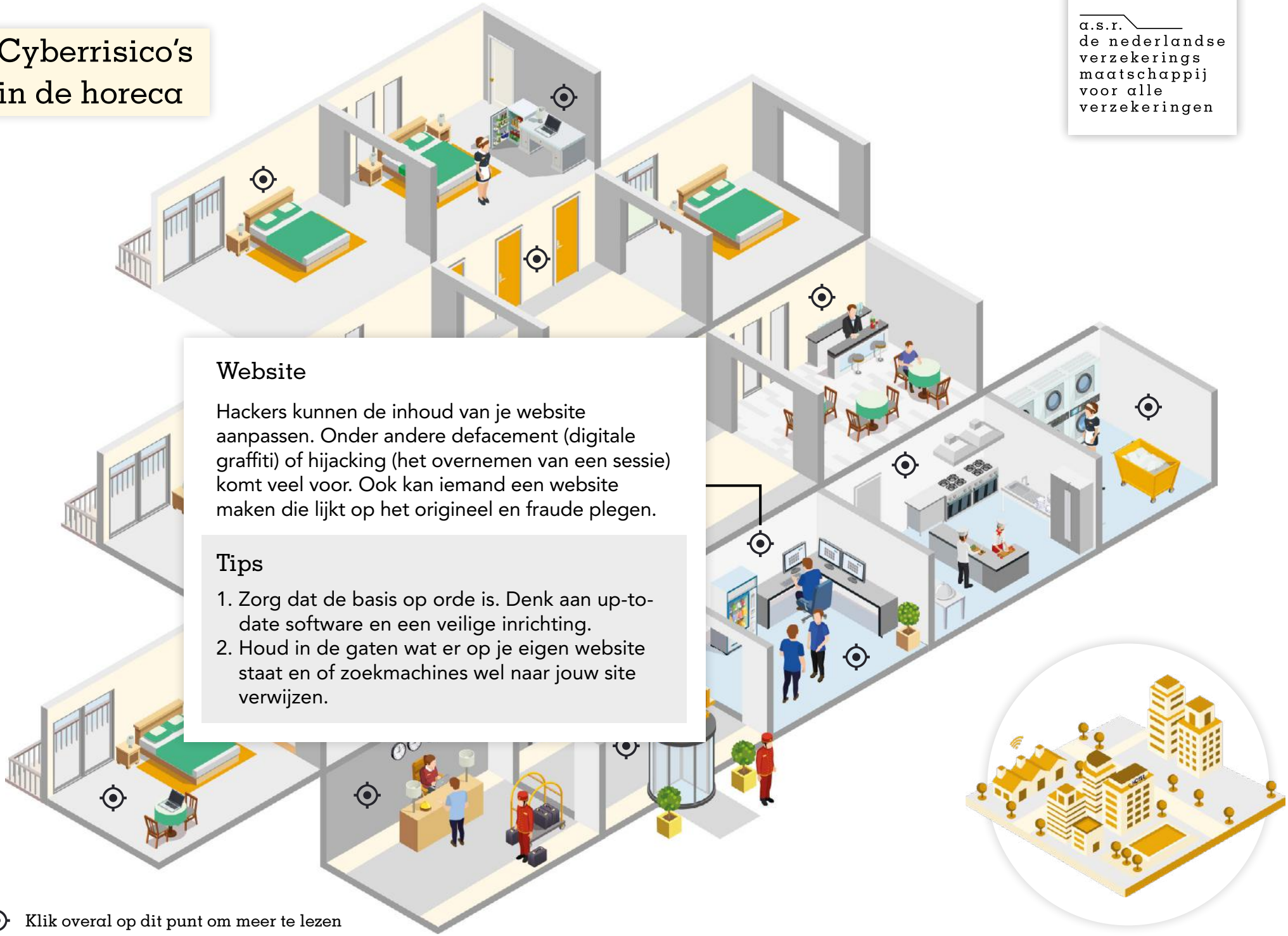
a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Website

Hackers kunnen de inhoud van je website aanpassen. Onder andere defacement (digitale graffiti) of hijacking (het overnemen van een sessie) komt veel voor. Ook kan iemand een website maken die lijkt op het origineel en fraude plegen.

Tips

1. Zorg dat de basis op orde is. Denk aan up-to-date software en een veilige inrichting.
2. Houd in de gaten wat er op je eigen website staat en of zoekmachines wel naar jouw site verwijzen.



Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

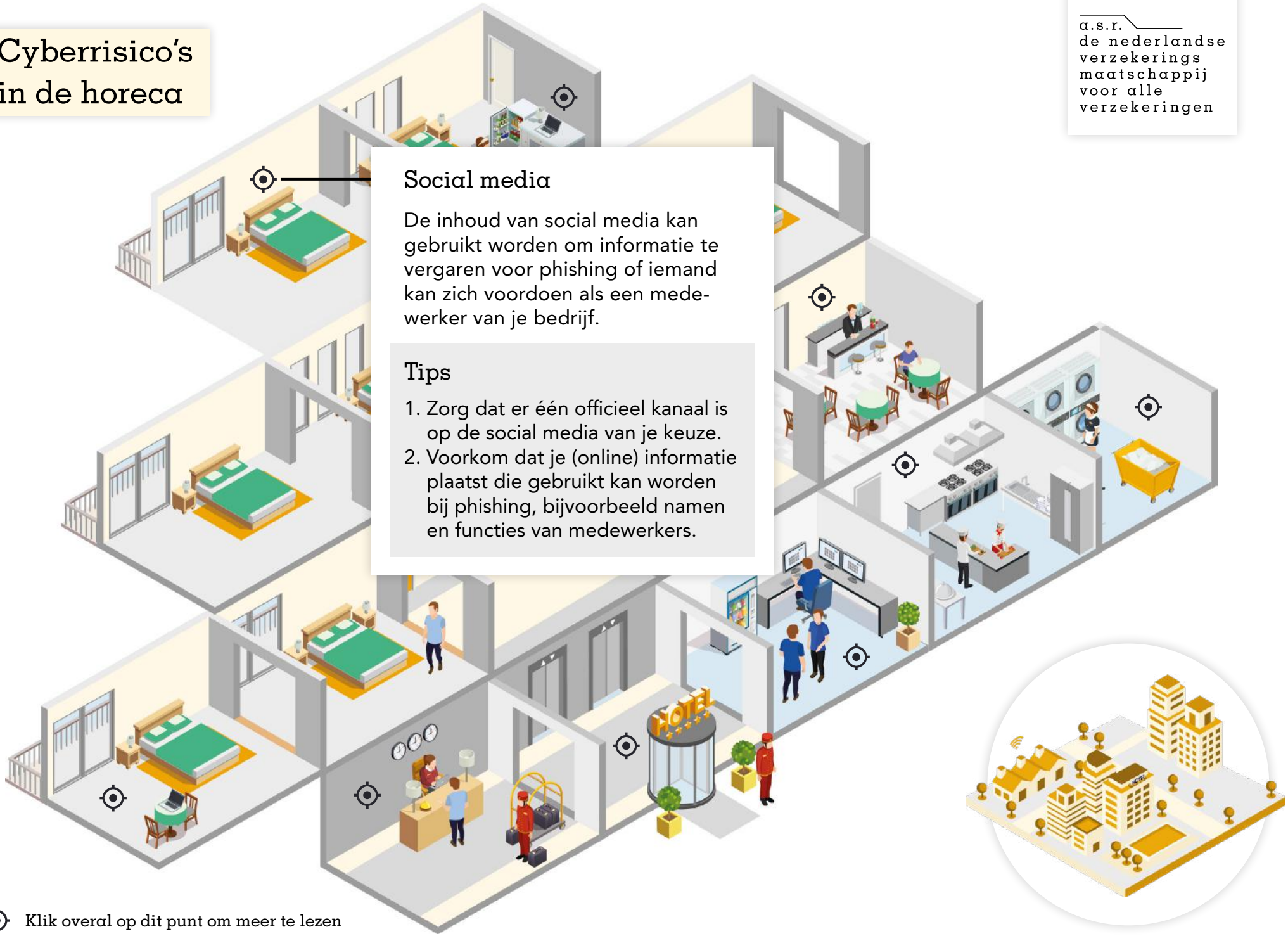
a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Social media

De inhoud van social media kan gebruikt worden om informatie te vergaren voor phishing of iemand kan zich voordoen als een mede-werker van je bedrijf.

Tips

1. Zorg dat er één officieel kanaal is op de social media van je keuze.
2. Voorkom dat je (online) informatie plaatst die gebruikt kan worden bij phishing, bijvoorbeeld namen en functies van medewerkers.



Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

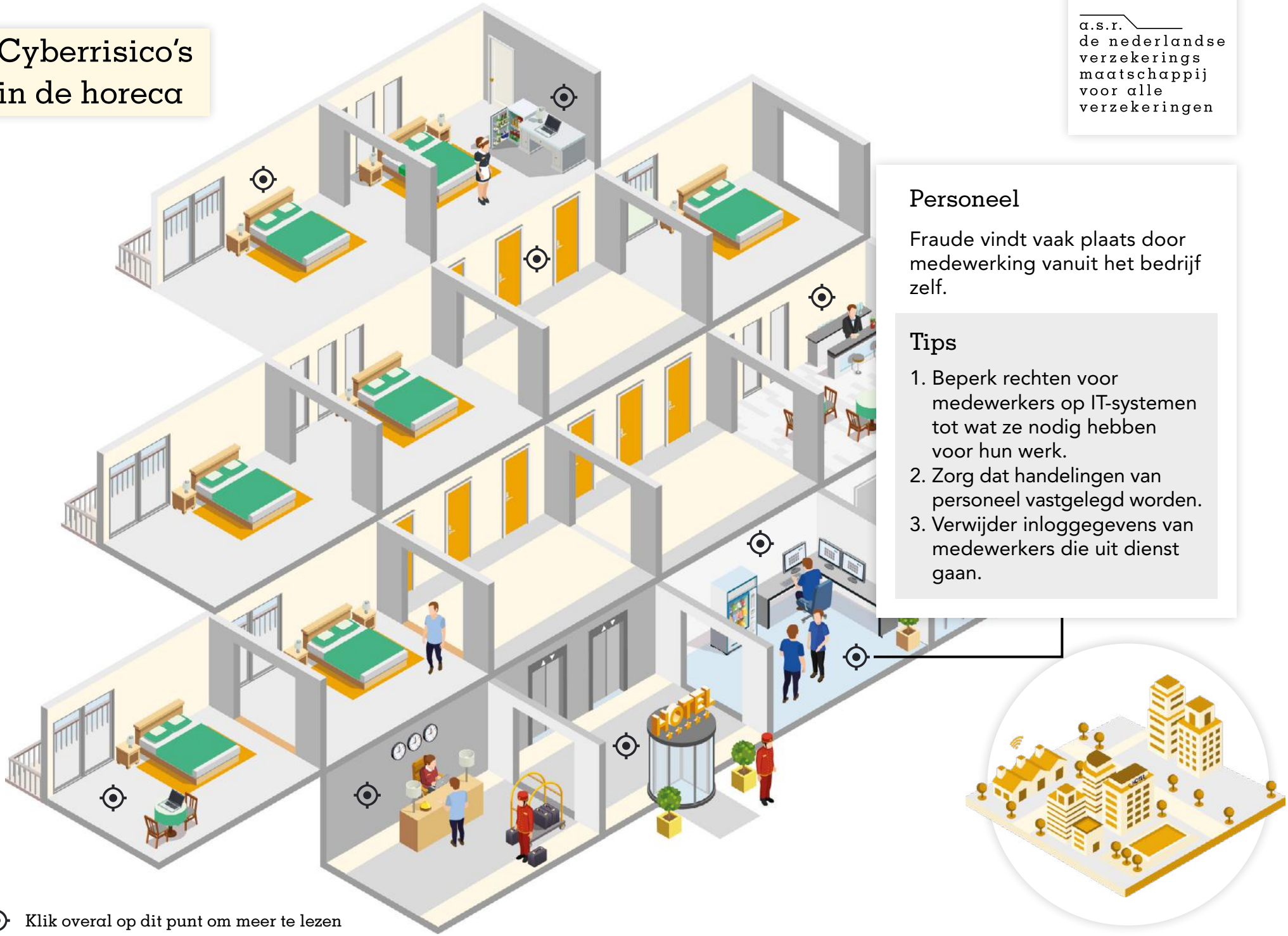
a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Personeel

Fraude vindt vaak plaats door medewerking vanuit het bedrijf zelf.

Tips

1. Beperk rechten voor medewerkers op IT-systemen tot wat ze nodig hebben voor hun werk.
2. Zorg dat handelingen van personeel vastgelegd worden.
3. Verwijder inloggegevens van medewerkers die uit dienst gaan.



Klik overal op dit punt om meer te lezen

Cyberrisico's in de horeca

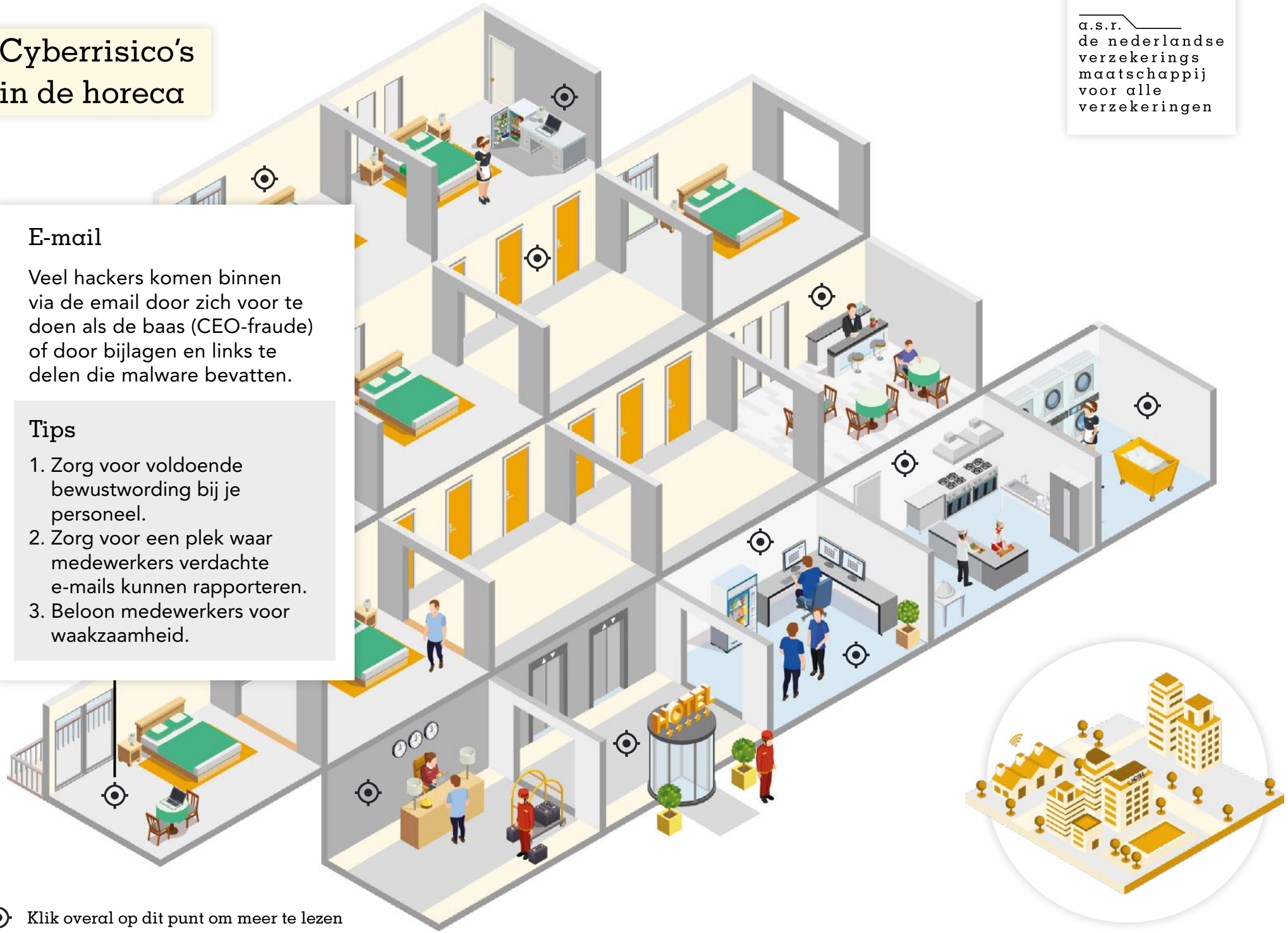
a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

E-mail

Veel hackers komen binnen via de email door zich voor te doen als de baas (CEO-fraude) of door bijlagen en links te delen die malware bevatten.

Tips

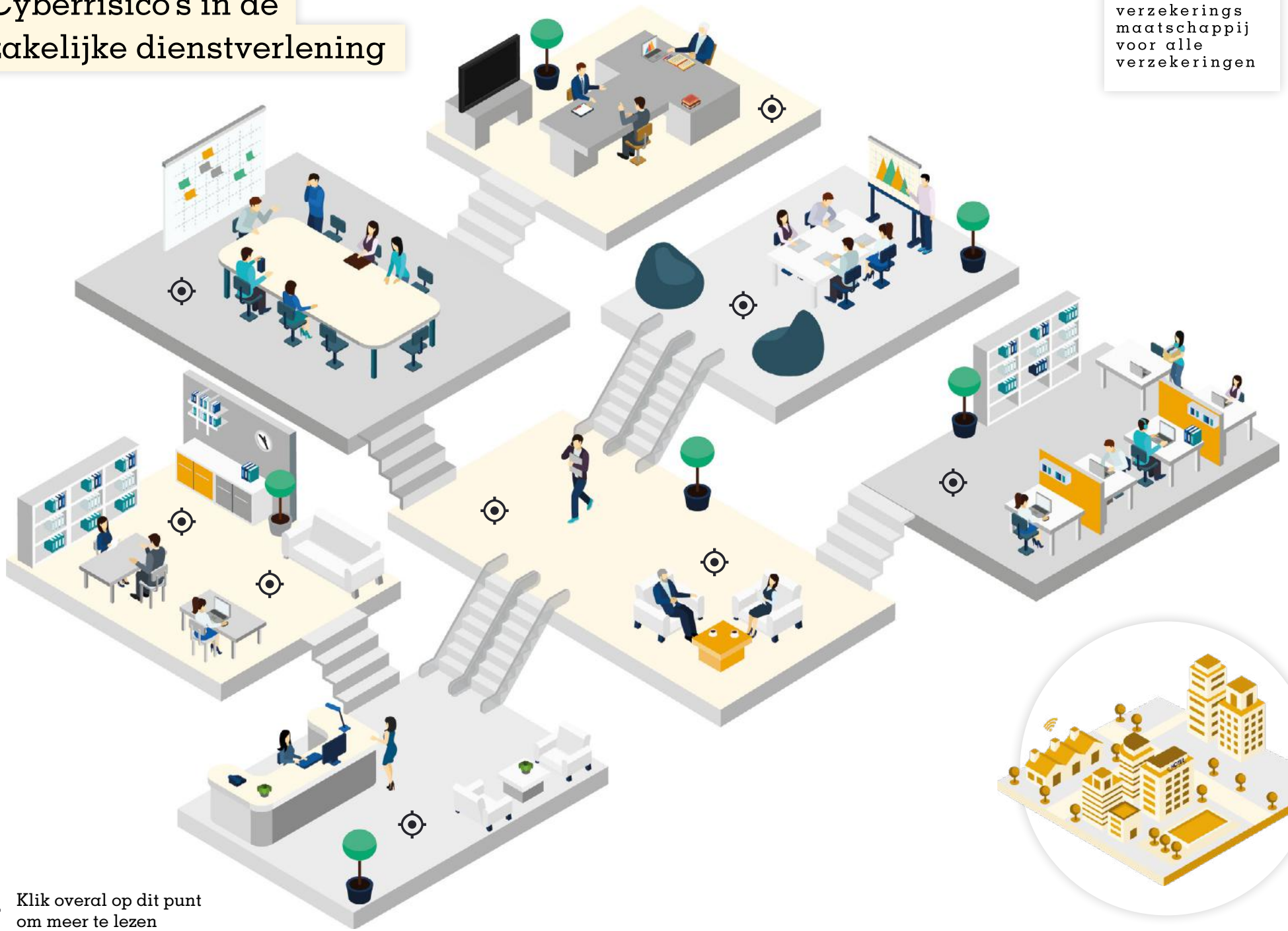
1. Zorg voor voldoende bewustwording bij je personeel.
2. Zorg voor een plek waar medewerkers verdachte e-mails kunnen rapporteren.
3. Beloon medewerkers voor waakzaamheid.



Klik overal op dit punt om meer te lezen

Cyberrisico's in de zakelijke dienstverlening

a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen



Klik overal op dit punt om meer te lezen

Cyberrisico's in de zakelijke dienstverlening

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Inkoop

Waar primaire en secundaire bedrijfsprocessen worden ondersteund door informatiesystemen en procedures is de digitale footprint groot. Het risico is kans op fraude binnen inkoop- en voorraadbeheerprocessen.

Tips

1. Draag zorg voor goede administratieve procedures rondom inkoopprocessen.
2. Beveilig de systemen die deel uitmaken van deze processen (Vulnerability & Patch Management).
3. Draag zorg voor de juiste autorisatie en controle van de gebruikte applicaties die een onderdeel zijn van de bedrijfsprocessen.

Klik overal op dit punt
om meer te lezen

Cyberrisico's in de zakelijke dienstverlening

a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

E-mail

Veel hackers komen binnen via de email door zich voor te doen als de baas (CEO-fraude) of door bijlagen en links te delen die malware bevatten.

Tips

1. Zorg voor voldoende bewustwording bij je personeel.
2. Zorg voor een plek waar medewerkers verdachte e-mails kunnen rapporteren.
3. Beloon medewerkers voor waakzaamheid.

Klik overal op dit punt om meer te lezen

Cyberrisico's in de zakelijke dienstverlening

a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Betalingen

Creditcardgegevens kunnen gestolen worden en bij 'skimming' worden bankpassen gekopiëerd.

Tips

1. Ga zorgvuldig om met creditcardgegevens, dieven zoeken er specifiek naar.
2. Voorkom dat betaalterminals onbeheerd toegankelijk zijn.

Klik overal op dit punt om meer te lezen

Cyberrisico's in de zakelijke dienstverlening

a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Camerabeveiliging

Camera's kunnen door buitenstaanders misbruikt worden om mee te kijken.

Tips

1. Zorg dat je camera's alleen via het interne netwerk of een VPN-verbinding te benaderen zijn.
2. Zorg dat elke camera een eigen wachtwoord heeft.
3. Werk regelmatig de software van de camera's bij.

Klik overal op dit punt om meer te lezen

Cyberrisico's in de zakelijke dienstverlening

a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Social media

De inhoud van social media kan gebruikt worden om informatie te vergaren voor phishing of iemand kan zich voordoen als een medewerker van je bedrijf.

Tips

1. Zorg dat er één officieel kanaal is op de social media van je keuze.
2. Voorkom dat je (online) informatie plaatst die gebruikt kan worden bij phishing, bijvoorbeeld namen en functies van medewerkers.

Klik overal op dit punt om meer te lezen

Cyberrisico's in de zakelijke dienstverlening

a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Personeel

Fraude vindt vaak plaats door medewerking vanuit het bedrijf zelf.

Tips

1. Beperk rechten voor medewerkers op IT-systemen tot wat ze nodig hebben voor hun werk.
2. Zorg dat handelingen van personeel vastgelegd worden.
3. Verwijder inloggegevens van medewerkers die uit dienst gaan.

Klik overal op dit punt om meer te lezen

Cyberrisico's in de zakelijke dienstverlening

a.s.r.
de nederlandse
verzekerings
maatschappij
voor alle
verzekeringen

Facturatie

Facturen bevatten vaak persoonsgegevens die gestolen kunnen worden of facturen kunnen aangepast worden.

Tips

1. Zorg dat facturen veilig opgeslagen en gedeeld worden.
2. Beveilig uitgaande digitale facturen tegen wijzigingen (readonly).
3. Match inkomende facturen met bekende debiteuren/open posten.

Klik overal op dit punt om meer te lezen

Cyberrisico's in de zakelijke dienstverlening

a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Dossierbehandeling

Risico op ongeautoriseerde toegang van klantgegevens met als impact AVG-boetes en reputatieschade.

Tips

1. Draag zorg voor goede administratieve procedures rondom dossierbehandelingprocessen.
2. Beveilig de systemen die deel uitmaken van deze processen (Vulnerability & Patch Management).
3. Draag zorg voor de juiste autorisatie en controle van de gebruikte applicaties die een onderdeel zijn van de bedrijfsprocessen.

Klik overal op dit punt om meer te lezen

Cyberrisico's in de zakelijke dienstverlening

a.s.r.
de nederlandse verzekerings maatschappij voor alle verzekeringen

Website

Hackers kunnen de inhoud van je website aanpassen. Onder andere defacement (digitale graffiti) of hijacking (het overnemen van een sessie) komt veel voor. Ook kan iemand een website maken die lijkt op het origineel en fraude plegen.

Tips

1. Zorg dat de basis op orde is. Denk aan up-to-date software en een veilige inrichting.
2. Houd in de gaten wat er op je eigen website staat en of zoekmachines wel naar jouw site verwijzen.

Klik overal op dit punt om meer te lezen