EUROPEAN
RENTAL
ASSOCIATION

SAMENVATTING

ERA-gids voor toonaangevende praktijken op het gebied van cyberbeveiliging in de sector materieelverhuur

Cyberbeveiliging — bent u toegerust voor de uitdaging?

Een van de grootste bedreigingen voor de materieelverhuursector is de kwetsbaarheid met betrekking tot de cyberbeveiliging van onze bedrijven. In 2021 bestaat er in onze sector geen routekaart aan de hand waarvan een verhuurbedrijf van materieel kan beoordelen waar het staat met betrekking tot cyberbeveiliging en kan bepalen welke toonaangevende praktijken het kan nastreven. Het doel van deze gids is om op ondernemingsniveau het toepassingsgebied van acties en maatregelen betreffende cyberbeveiliging te definiëren, de kernelementen van een succesvolle strategie vast te stellen, waaronder de specifieke factoren die van invloed kunnen zijn op verhuurbedrijven, en een overzicht te geven van toonaangevende praktijken die heden worden toegepast door de leiders in onze sector. Deze gids is samengesteld met de waardevolle steun en bijdragen van bedrijven die lid zijn van ERA.

De huidige bedreiging van cyberbeveiliging en de “oproep tot actie”

In deze gids wordt beschreven hoe de sector materieelverhuur in heel Europa te maken heeft met een ongekende uitdaging wat betreft de bedreigingen die uitgaan van kwetsbaarheden en blootstellingen op het gebied van informatietechnologie in onze activiteiten, en met name hoe klanten steeds meer van ons eisen in verband met bescherming tegen cybercriminaliteit. De sector bevindt zich in een proces van consolidatie, waarbij kleinere bedrijven met andere ondernemingen fuseren om schaalgrootte te bereiken, en grotere bedrijven de kleinere overnemen om nieuwe markten te betreden, om zich te versterken of om aan marktaandeel te winnen. De verhuursector omarmt momenteel de “digitalisering”. Meer online zijn betekent meer risico’s op het gebied van cyberveiligheid. De verhuur van materieel wordt steeds intelligenter en meer verbonden met netwerken, die een aanvalskanaal kunnen zijn. Bedrijven die materieel verhuren en een ernstig incident hebben ondergaan, hebben het gevoel dat ze hun bedrijf, hun reputatie en vooral hun klanten en belanghebbenden in groot gevaar hebben gebracht. De EU-wetgeving wordt steeds strenger en in de gids wordt gewezen op de meest recente ontwikkelingen in de richtlijn inzake netwerk- en informatietechnologie (NIB) van de EU. De sector heeft nu behoefte aan een permanente gemeenschap van Europese bedrijven om samen te werken aan beste praktijken op het gebied van cyberbeveiliging, gemeenschappelijke bedreigingen en problemen waarmee alle organisaties te kampen hebben.

Budgettering van en investeringen in cyberbeveiliging

In deze gids worden de investeringen in en de kosten van een goede cyberbeveiliging toegelicht. Er wordt een investeringsschaal en een “maturiteit” getoond, waar de aanvankelijke investering om een basis te leggen wordt aangegeven.
Goede cyberbeveiliging vereist aanzienlijke investeringen – en moet ieder jaar worden vernieuwd. Rechtstreekse investeringen in cyberbeveiliging bedragen in alle sectoren circa 5% van de IT-uitgaven, en zijn bij aanvang nog hoger. Leidinggevende bedrijven geven ook aan dat de grootste investeringen worden gedaan in de indirecte en immateriële kosten van het “op maat maken”, beheren en verankeren van beveiliging in alles wat ze doen, wat uiteindelijk meer kan bedragen dan de directe kosten.

Routekaart van toonaangevende praktijken en checklist

De aandacht voor maatregelen op het gebied van cyberbeveiliging is vaak gericht op technologie en systemen, maar veel risico's hebben hun oorsprong in menselijk gedrag, in de robuustheid van de processen en in monitoring, rapportage en respons binnen het bedrijf. Volgens de leiders op dit gebied moet een organisatie een strategie op het niveau van de hele onderneming overwegen om ervoor te zorgen dat alle gebieden van kwetsbaarheid in

aanmerking worden genomen. Elke organisatie heeft verschillende risico's, werkterreinen en lacunes, maar volgens de leiders kan een checklist voor een allesomvattend toepassingsgebied worden ondergebracht in vier capaciteitsonderdelen die betrekking hebben op processen, mensen, technologie en infrastructuur. Deze worden in de gids geanalyseerd en er worden kernvereisten voor capaciteiten op drie niveaus gepresenteerd: “basisniveau”, “maturiteit” en “leider”. De gids omvat een checklist die de essentiële risico- en kwetsbaarheidsbeoordeling koppelt aan de huidige maturiteitsniveaus in het bedrijf, als hulpmiddel bij de planning en risicobeperking.

“*Je krijgt wat je meet...”* Volgens de leidende ondernemingen is het essentieel om ervoor te zorgen dat de belangrijkste prestatiegebieden die van invloed zijn op cyberbeveiliging worden gemeten met kritieke prestatie-indicatoren (KPI's). De routekaart in de gids geeft vervolgens typische maatregelen en prestatiemetingssystemen aan die tegenwoordig door toonaangevende bedrijven voor elk van de onderdelen worden gebruikt.

Toelichting van toonaangevende praktijken

In de gids worden enkele toonaangevende praktijken geïllustreerd die heden worden gebruikt voor de vier capaciteitsonderdelen. De leidende ondernemingen benadrukken dat, hoewel een alomvattend veiligheidsplan een essentieel onderdeel is van een alomvattende strategie, een overkoepelend plan niet de eerste stap hoeft te zijn – een volledig plan kan normaal gesproken in maturiteitsfasen tot stand komen. De belangrijkste kenmerken zijn:

- **Proces**: leiders benadrukken dat het in een vroeg stadium belangrijker is om stappen te ondernemen om alle mogelijke gebieden met een hoog risico in het bedrijf te identificeren en prioriteit te geven aan acties om kwetsbare punten te dichten of te patchen. Een uitgebreide scan van de risico's in elk van de pijlergebieden in deze gids kan een goed startpunt zijn. Op het moment dat gebieden met een hoog risico worden opgelost, kunnen gebieden met een matig risico worden aangepakt. Uit onderzoek blijkt dat het proces vanaf een basisniveau drie tot vijf jaar kan vergen om alle belangrijke risicogebieden te bestrijken, waarvoor aanzienlijke en voortdurende investeringen nodig zijn. Leiders wijzen op een “basic, better, best”-type traject om een op het doel afgestemde beveiliging te bereiken, waarbij formele accreditaties zoals mijlpalen kunnen worden gebruikt of waarbij de beveiliging intern op maat wordt gemaakt en dezelfde beginselen worden gevolgd. Er wordt een aantal in gebruik zijnde internationale kaders beschreven.

- **Mensen:** *cybersecurity is geen “IT-ding*”... Er is een belangrijke rol weggelegd voor Human Resources Management (HR) op het gebied van cyberveiligheid. De reikwijdte van HR-interventie en -ondersteuning in toonaangevende ondernemingen beslaat de hele onderneming en omvat het ontwerp en de ontwikkeling van beleid en procedures (waaronder de AVG- en gegevensbeschermingsprotocollen) en de bekendmaking daarvan aan alle werknemers, de aanpassing van de arbeidsvoorwaarden en rolbeschrijvingen van werknemers om daarin verantwoordelijkheden op het gebied van gegevens en beveiliging op te nemen, de bewustmaking van en opleiding over cyberbeveiligingsgeisen en een analyse van opleidingsbehoeften voor eerstelijnsfuncties en specifiek beveiligingspersoneel. Communicatiemiddelen zoals nieuwsbrieven of bulletins in de sociale media om de laatste trends of bedreigingen in de hele onderneming bekend te maken, zijn van essentieel belang.

- **Technologie:** de instrumenten van informatietechnologie blijven zich snel ontwikkelen en bieden een krachtig middel voor cyberverdediging, voor een “vroegtijdige waarschuwing” en het onderscheppen van bedreigingen. Monitoring van bedreigingen en gezondheid wordt mogelijk gemaakt door technologie met geavanceerde systemen zoals “Splunk” en “MS Azure Sentinel”, waarvan het gebruik wordt geïllustreerd. De oprichting van een “SOC” (Security Operations Centre) wordt essentieel geacht om automatische systemen optimaal te benutten. Leiders kunnen een intern SOC hebben, dat vaak wordt aangevuld met centra van derden die 24/7 ondersteuning en geavanceerde monitoring- en managementdiensten kunnen bieden.

- **Infrastructuur:** *“Als het ergste gebeurt, moet je, ondanks de beste preventiemaatregelen, klaar staan met een incidentenbeheersplan.”* Aanvallen kunnen in vele vormen voorkomen, maar een van de ernstigste soorten is een “ransomware-aanval”. In geval van een denial-of-service van het systeem is een onmiddellijke noodrespons vereist, maar er moet een proces zijn opgezet om de situatie te beoordelen en te “triëren”. Deze gids illustreert hoe leidende bedrijven analyseren en reageren en biedt een “eerste 48-uur”-model, dat kan bijdragen aan de planning van de crisisbeheersingsperiode onmiddellijk na een denial-of-service-voorval of een andere grote

storing.

Neem maatregelen voor een veilige toekomst

De race naar goede IT-beveiliging zal nooit eindigen, maar om voorop te blijven, moeten materieelverhuurbedrijven volgens de leiders het volgende doen:

1. *Hun capaciteiten, sterke punten en kwetsbaarheden kennen*
2. *Een risicobeoordeling uitvoeren*
3. *Op de juiste manier plannen en investeren*
4. *Voorbereid zijn, voor het geval het ergste gebeurt*
5. *Vernieuwen en voortdurend verbeteren*

De “ERA-gids voor toonaangevende praktijken op het gebied van cyberbeveiliging” is bedoeld om verhuurbedrijven van materieel van ieder type en omvang te helpen bij het plannen, ontwikkelen of voortdurend verbeteren van hun cyberbeveiliging.