EUROPEAN
RENTAL
ASSOCIATION

KURZFASSUNG
ERA-Leitfaden für führende Cybersicherheits-Praktiken in der Baumaschinen- und Gerätevermietbranche

Cybersicherheit - sind Sie für die Herausforderung gewappnet?

Eine der größten Bedrohungen für die **Vermietbranche** ist die Anfälligkeit für Cybersicherheits-Auswirkungen auf unsere Unternehmen. Im Jahr 2021 gibt es in unserer Branche keinen etablierten Wegweiser, anhand dessen ein Baumaschinen- und Gerätevermieter bewerten kann, wo es in Bezug auf die Cybersicherheit steht und führende Praktiken ausmachen kann, die es umsetzen kann. Der Zweck dieses Leitfadens ist es, den unternehmensweiten Geltungsbereich von Cybersicherheitsmaßnahmen zu definieren und die Kernelemente einer erfolgreichen Strategie zu ermitteln, einschließlich der besonderen Faktoren, die sich auf Vermietunternehmen auswirken können, und führende Praktiken zu skizzieren, die heute von Marktführern in unserer Branche angewendet werden. Dieser Leitfaden wurde mit der wertvollen Unterstützung und den Beiträgen der ERA-Mitgliedsunternehmen erstellt.

Die heutige Bedrohung der Cybersicherheit und die "Handlungsaufforderungen"

Dieser Leitfaden beschreibt, wie die Vermietbranche in ganz Europa vor einer noch nie dagewesenen Herausforderung stellt, was die Bedrohungen durch informationstechnische Schwachstellen und Gefährdungen in unserem Geschäft angeht, und wie insbesondere die Kundschaft in Bezug auf Cybersicherheit immer höhere Anforderungen von uns fordert. Die Branche befindet sich in einem Konsolidierungsprozess, bei dem kleinere Unternehmen mit anderen fusionieren, um Größenvorteile zu erzielen und größere Unternehmen kleinere Unternehmen aufkaufen, um neue Märkte zu erschließen, zu konsolidieren oder Marktanteile zu gewinnen. Die Bau- und Gerätevermietbranche macht sich die "Digitalisierung" zu eigen. Die Zunahme des „Onlinegeschäfts“ bedeutet mehr Bedrohungen der Cybersicherheit. Mietgeräte werden immer intelligenter und sind mit Netzwerken verbunden, die als Einfallstor für Angriffe dienen können. Gerätevermieter, die einen bedrohlichen Vorfall erlebt haben, merken, dass sie ihr Geschäft, ihren Ruf und vor allem ihre Kunden und Stakeholder einem hohen Risiko ausgesetzt haben. Die EU-Gesetzgebung nimmt an Intensität zu, und der Leitfaden verweist auf die jüngsten Entwicklungen in der NIS-Richtlinie (Netz- und Informationssicherheit) der EU. Die Branche braucht nun eine ständige Gemeinschaft europäischer Unternehmen, um an bewährten Verfahren der Cybersicherheit, gemeinsamen Bedrohungen und Problemen aller Organisationen zusammenzuarbeiten.

Cybersicherheits-Budgetierung und Investitionsbedarf

Dieser Leitfaden veranschaulicht die Investitionen und die Kosten für eine angemessene Cybersicherheit. Präsentiert wird eine Investitions- und "Reifeskala", welche die Anfangsinvestitionen für die Schaffung der Grundlagen angibt. Gute Cybersicherheit erfordert erhebliche Investitionen - und muss jedes Jahr erneuert werden. Die direkten Investitionen in die Cybersicherheit werden über alle Branchen hinweg mit etwa 5 % der IT-Ausgaben angegeben, wobei die Anfangsinvestitionen höher sind. Marktführer zeigen auch, dass die größeren Investitionen in den indirekten und immateriellen Kosten für das "Design-In", das Management und die Einbettung von Sicherheit in alles, was sie tun, liegen, die sich letztendlich auf mehr als die direkten Kosten belaufen können.

Wegweiser der führenden Praktiken und "Checkliste"

Der Fokus bei Eingriffen zur Cybersicherheit liegt oft auf Technologie und Systemen, doch viele Risiken haben ihre Ursache im menschlichen Verhalten, der Robustheit von Prozessen und der Überwachung, Berichterstattung und Reaktion innerhalb des Unternehmens. Laut den führenden Bau- und Gerätevermietern muss eine Organisation in diesem Bereich eine unternehmensweite Strategie in Betracht ziehen, um sicherzustellen, dass alle anfälligen Bereiche berücksichtigt werden. Jede Organisation wird unterschiedliche Risiken, operative Rahmen und Lücken

aufweisen, jedoch sind die Marktführer der Meinung, dass eine Checkliste für einen umfassenden Rahmen mit vier Fähigkeitselementen erfasst werden kann, die Prozesse, Menschen, Technologie und Infrastruktur abdecken. Daher werden sie in diesem Leitfaden analysiert und die Kernfähigkeitsanforderungen auf jeder der drei Ebenen "Basis-Level", "Reif" und "Leader" dargestellt. Es ist eine Checkliste enthalten, die, als Hilfe für die Planung und Risikominderung, die wesentliche Risiko- und Schwachstellenbewertung mit dem aktuellen Reifegrad im Unternehmen verbindet.

"*Man bekommt, was man misst.....*" Marktführer berichten, wie wichtig es ist, sicherzustellen, dass Leistungs-Schlüsselbereiche, die sich auf den Cybersicherheitsstatus auswirken, mit Leistungskennzahlen oder Key Performance Indicators (KPIs) gemessen werden. Im Wegweiser des Leitfadens werden typische Maßnahmen und Systeme zur Leistungsmessung aufgeführt, die heute von führenden Unternehmen für jedes der Elemente verwendet werden.

Veranschaulichung führender Praktiken

Dieser Leitfaden veranschaulicht schließlich einige der führenden Praktiken, die heute im Hinblick auf die vier Fähigkeitselemente verwendet werden. Marktführer betonen, dass ein umfassender Sicherheitsplan zwar ein wesentlicher Bestandteil einer umfassenden Strategie ist, aber ein übergreifender Plan nicht der allererste Schritt sein muss - ein vollständiger Plan kann typischerweise nach Reifestufen entstehen. Zu den Schlüssel-Merkmalen gehören:

- **Prozess**: Marktführer betonen, dass es in der Anfangsphase wichtiger ist, Maßnahmen zu ergreifen, um alle möglichen risikoreichen Bereiche im Unternehmen zu identifizieren und Maßnahmen zu priorisieren, um Schwachstellen zu schließen oder zu beheben. Ein umfassendes Scannen der Risiken in jedem der Bereiche dieses Leitfadens kann ein guter Ausgangspunkt sein. Sobald die Bereiche mit hohem Risiko abgearbeitet sind, können die Bereiche mit mittlerem Risiko in Angriff genommen werden. Es ist wichtig, Untersuchungen zu erwähnen, die darauf hindeuten, dass es ein drei- bis fünfjähriger Prozess sein kann, ausgehend von einem Basisniveau alle wesentlichen Risikobereiche abzudecken, was erhebliche und anhaltende Investitionen erfordert. Marktführer suchen sich den Weg aus einer grundlegenden, guten oder besten Art aus, zu einer zweckmäßigen Sicherheit, wobei formale Akkreditierungen als Meilensteine genutzt werden können oder der Prozess im eigenen Haus entwickelt werden kann, jeweils den gleichen Prinzipien folgend. Es werden eine Reihe von internationalen Orientierungsrahmen skizziert, die im Einsatz sind.

- **Menschen:** *Cybersicherheit ist keine "IT-Angelegenheit"...* Das Personalmanagement (HR) spielt bei der Verteidigung der Cybersicherheit eine wichtige Rolle. Der Umfang der HR-Intervention und -Unterstützung in Marktführer-Unternehmen erstreckt sich auf das ganze Unternehmen und umfasst die Gestaltung und Entwicklung von Richtlinien und Verfahren (einschließlich DSGVO- und Datenschutzprotokollen) und deren Kommunikation an alle Mitarbeiter, die Anpassung von Arbeitsbedingungen und Rollenbeschreibungen, um Daten- und Sicherheitsverantwortlichkeiten einzubeziehen, die Sensibilisierung und Schulung für die Erfordernisse der Cybersicherheit und die Analyse des Schulungsbedarfs für führende Positionen und spezifisches Sicherheitspersonal. Kommunikationsmedien wie Newsletter oder Social-Media-Nachrichten zur Verbreitung der neuesten Trends oder Bedrohungen im gesamten Unternehmen sind unerlässlich.

- **Technologie:** Tools der Informationstechnologie entwickeln sich rasant weiter und bieten ein leistungsfähiges Mittel zur Cybersicherheit, zur "Frühwarnung" und zum Abfangen von Bedrohungen. Bedrohungs- und Zustandsüberwachung wird durch Technologien wie "Splunk" und "MS Azure Sentinel", die im Einsatz gezeigt werden, ermöglicht. Die Einrichtung eines "SOC" (Security Operations Centre/Sicherheit-Operations-Center) wird, um die Leistungsfähigkeit der automatisierten Systeme optimal zu nutzen, als essenziell dargestellt. Führende Unternehmen können ein internes SOC betreiben, das oft durch Zentren von Drittanbietern ergänzt wird, die einen 24x7-Support und erweiterte Überwachungs- und Managementdienste anbieten können.

- **Infrastrukturen: "***Wenn trotz aller besten Präventionsmaßnahmen das Schlimmste passiert, müssen Sie mit einem Störfallmanagement-Plan vorbereitet sein."* Angriffe können in vielen Formen auftreten, aber eine der gefährlichsten kann ein "Ransomware-Angriff" sein. In einer Systemsperrungssituation ist eine sofortige

Notfallreaktion erforderlich, aber es muss ein Prozess zur Bewertung und "Zuordnung" der Situation eingerichtet worden sein. Dieser Leitfaden veranschaulicht, wie Marktführer die Situation analysieren und auf sie reagieren, und bietet eine "Erste 48"-Vorlage, die bei der Planung des Krisenmanagements unmittelbar nach einer Systemsperre-Situation oder einer anderen größeren Ausfallbedrohung helfen kann.

Vorbereitung für eine sichere Zukunft

Der Wettlauf um eine gute IT-Sicherheit wird nie enden, aber um stets ganz vorne dabei zu sein, fordern die Marktführer, dass Baumachinen- und Gerätevermieter:

1. *ihre Vorteile, Stärken und Schwachstellen kennen,*
2. *eine Risikoanalyse durchführen,*
3. *angemessen planen und investieren,*
4. *für den „Worst Case“ vorbereitet sind,*
5. *kontinuierlich verbessern und aktualisieren.*

Der "ERA Guide to Cybersecurity Leading Practice/ERA Leitfaden zur führenden Cybersicherheits-Praxis" soll Baumachinen- und Gerätevermietunternehmen aller Arten und Größen helfen, ihre Cybersicherheit zu planen, zu entwickeln, beziehungsweise kontinuierlich zu verbessern.