G06715
15.8.2024
Nr. 16

sicherheits.berater

Informationsdienst für Sicherheit in Wirtschaft und Verwaltung

295 ›››

Vision Zero: ambitioniert oder unrealistisch?

Zweite Seite

Warnung vor russischer Spionage und Sabotageakten

Liebe Leserinnen und Leser,

im „Sicherheitshinweis für die Wirtschaft“ vom 26. Juli 2024 warnt das Bundesamt für Verfassungsschutz davor, allzu leichtfertig mit der Veröffentlichung von Informationen umzugehen: Solche Infos könnten von ausländischen Nachrichtendiensten ausgekundschaftet werden. Namentlich genannt werden die russischen Nachrichtendienste, von denen eine erhöhte Gefährdung durch Sabotageaktivitäten bzw. entsprechende Vorbereitungshandlungen in Deutschland ausgehe. Vor allem russischsprachige Beschäftigte könnten in deren Blickfeld rücken. Das Bundesamt veröffentlichte dazu auch entsprechende Handlungsempfehlungen zur Prävention.

Das Bundesamt für Verfassungsschutz weist noch einmal darauf hin, dass Nachrichtendienste und auch andere Tätergruppierungen gezielt offen zugängliche Informationen auswerten und in Handlungsempfehlungen, z. B. zu Sabotage- und Anwerbungszwecken, an ihre operativen Kräfte einfließen lassen. Insbesondere russischsprachige oder pro-russische Beschäftigte und solche, die sich in den sozialen Medien öffentlich eindeutig für oder gegen die Ukraine-Unterstützung des Westens positionieren, könnten ins Blickfeld russischer Nachrichtendienste rücken und sich mit Rekrutierungsversuchen konfrontiert sehen. Auch könnten Objekte zum Ziel russischer Nachrichtendienste werden, deren strategische Bedeutung für Russland sich nicht unmittelbar erschließt. Mit dieser Warnung geht das BfV übrigens konkret nicht so weit wie der auf das Thema Prospective Intelligence spezialisierte Sicherheitsberater Florian Peil, der mit Verweis auf den Vorfall um Rheinmetall-CEO Papperger auch vor Mordanschlägen warnt (www.florianpeil.de).

Im aktuellen „Sicherheitshinweis für die Wirtschaft“ vom 26. Juli 2024 zählt das BfV einige Handlungsempfehlungen auf, deren Lektüre wir empfehlen (www.verfassungsschutz.de, Kurzlink https://tinyurl.com/6vftayz6). Dazu gehört z. B. der Punkt, besonders gefährdete Mitarbeiter entsprechend für Gefahren zu sensibilisieren, sodass relevante Vorkommnisse gemeldet werden. Auch den Personalverantwortlichen in den Unternehmen schreibt der Verfassungsschutz Prävention ins Stammbuch: So sei bei Stellenausschreibungen kritisch abzuwägen, welche Informationen zwingend veröffentlicht werden müssten. Angreifer könnten schließlich durch bestimmte Informationen abschätzen, mit welchen Sicherheitssystemen, mit welcher Sicherheitssoftware oder mit welchem industriellen Kontrollsystem (ICS) sie es zu tun hätten. Darüber hinaus empfiehlt der Verfassungsschutz Maßnahmen zur Sicherheitskonzeption, z. B. die Investition in eine angemessene Zaunanlage, Kameraüberwachung und einen Wachschutz, das Härten von Übermittlungswegen durch Zwei-Faktor-Authentifizierung, das Durchführen von Penetrationstests bis hin zu dem Tipp, möglichst eine Verschleierung der eigenen IP-Adressen zu ermöglichen.

Das BfV bietet Unternehmen weitere Hilfen an: wirtschaftsschutz@bfr.bund.de bzw. +49 30 18792-3322.

Der Autor Bernd Zimmermann
Magister Artium (Politikwissenschaft)

Chefredakteur Sicherheits-Berater, Security Engineer BdSI

ARBEITSSICHERHEIT

Vision Zero: ambitioniertes Ziel oder unrealistischer Druck?

Vision Zero ist ein Konzept, das darauf abzielt, alle arbeitsbedingten Unfälle und Erkrankungen zu eliminieren. Das zentrale Prinzip von Vision Zero ist die Überzeugung, dass jeder Unfall vermeidbar ist und dass das Ziel von null Unfällen daher realistisch und erreichbar ist. Das Konzept basiert auf der ethischen Verantwortung, jedem Menschen eine sichere Arbeitsumgebung zu gewährleisten. Arbeitgeber und Führungskräfte tragen die Verantwortung, diese Sicherheit zu ermöglichen. Der Ansatz setzt auf Prävention und geht davon aus, dass durch proaktive Maßnahmen und eine systematische Gefährdungsbeurteilung Risiken minimiert werden können. Dabei spielt auch die kontinuierliche Verbesserung der Sicherheitsmaßnahmen eine zentrale Rolle. Das Lernen aus Beinahe-Unfällen und regelmäßige Sicherheitsaudits sind entscheidend, um die Sicherheitsstandards stets zu optimieren. Ein weiterer wichtiger Aspekt ist die Einbindung der Mitarbeiter in die Sicherheitsprozesse. Durch ihre aktive Beteiligung und kontinuierliche Schulung können Unternehmen die Arbeitssicherheit effektiv verbessern.

Die Deutsche Gesetzliche Unfallversicherung (DGUV) bietet diesbezüglich einen guten Überblick mit weiteren Links (zuletzt aufgerufen am 16.7.2024): dguv.de, Kurzlink: tinyurl.com/ykhkn6uc . Eine der führenden globalen Organisationen für soziale Sicherheit ist die International Social Security Association (ISSA). Diese hat ebenfalls konkrete Handlungsempfehlungen zum Thema Vision Zero veröffentlicht. Hier ein Link und Empfehlungen für die Energiewirtschaft: issa.int, Kurzlink https://tinyurl.com/2p825ekh .

Strategien und Maßnahmen

Um Vision Zero in die Praxis umzusetzen, sollten die Unternehmen laut den oben genannten Quellen verschiedene Strategien und Maßnahmen ergreifen:

- **Sicherheitskultur etablieren**
  Sicherheit muss als zentraler Wert im Unternehmen verankert werden. Führungskräfte müssen eine Vorbildfunktion übernehmen und die Bedeutung der Arbeitssicherheit aktiv kommunizieren.

» Der Ansatz setzt auf Prävention. «

- **Risikobewertung und Gefahrenanalyse**
  Durch regelmäßige Analysen können potenzielle Gefahren identifiziert und beseitigt werden. Dies beinhaltet sowohl proaktive als auch reaktive Maßnahmen.

- **Technologische Innovationen nutzen**
  Moderne Technologien wie Automatisierung, Robotik und tragbare Sensoren können die Arbeitssicherheit erheblich verbessern. Virtuelle Realität (VR) kann für realitätsnahe Sicherheitstrainings genutzt werden.

- **Beteiligung der Mitarbeiter fördern**
  Mitarbeiter sollten aktiv in die Entwicklung und Umsetzung von Sicherheitsmaßnahmen einbezogen werden. Eine offene Kommunikationskultur ist hierbei entscheidend.

Kritische Aspekte der Vision

Trotz der positiven Intentionen und der theoretischen Machbarkeit von Vision Zero gibt es auch kritische Aspekte, die beachtet werden müssen:

- **Erwartungshaltung und Druck**
  Das Ziel, null Unfälle zu erreichen, kann zu einem hohen Erwartungsdruck führen. Mitarbeiter und Führungskräfte könnten sich gezwungen fühlen, Unfälle und Fehler

zu verschweigen, um die Zielvorgaben zu erfüllen. Dies kann zu einer Kultur des Vertuschens führen, in der Ursachen von Unfällen nicht offen angesprochen und analysiert werden.

- Realitätsferne Ziele
  In bestimmten Branchen und Arbeitsumgebungen, in denen Risiken besonders hoch sind, kann das Ziel von null Unfällen als unrealistisch wahrgenommen werden. Dies kann zu Frustration und Demotivation führen.

- Fehlende Fehlerkultur
  Eine offene Fehlerkultur ist essenziell für kontinuierliche Verbesserungen. Wenn jedoch die Angst vor Sanktionen überwiegt, werden Fehler möglicherweise nicht mehr gemeldet und somit auch nicht analysiert und behoben.

- Ressourcenaufwand
  Die Implementierung von Vision Zero erfordert erhebliche Ressourcen in Form von Zeit, Geld und Engagement. Kleine und mittelständische Unternehmen könnten Schwierigkeiten haben, diese Ressourcen bereitzustellen.

Erwartungsdruck und Realismus

Fazit

Vision Zero ist ein ehrgeiziges und lobenswertes Ziel, das eine sicherere Arbeitsumgebung fördern soll. Dennoch sollten Unternehmen bedenken, dass die Erreichung dieses Ziels oft mit einem erheblichen Erwartungsdruck und potenziellen negativen Folgen verbunden ist. Anstatt Vision Zero als eigenständiges Ziel auszurufen, könnten Unternehmen besser beraten sein, sich auf bewährte Maßnahmen wie Gefährdungsbeurteilungen, eine offene Fehlerkultur, Analyse und Bewertung von Beinahe- und tatsächlichen Unfällen und regelmäßigen Unterweisungen zu konzentrieren. Diese Ansätze fördern ebenfalls eine sichere Arbeitsumgebung, ohne den zusätzlichen Druck eines möglicherweise unrealistischen Ziels zu erzeugen. Durch die konsequente Anwendung dieser bewährten Methoden können Unternehmen die Arbeitssicherheit effektiv verbessern und gleichzeitig eine gesunde, transparente und fehlerfreundliche Unternehmenskultur aufrechterhalten.

Der Autor Fabian Hecker
Bachelor of Science (Safety & Security Engineering)

Sicherheitsberater, Redaktionsmitglied des Sicherheits-Berater (seit 2016) mit den Spezialgebieten Videokonzeption, Leitstellenplanung, Sicherheitssysteme und Sicherheitskonzepte

SICHERHEITSZENTRALEN

Checkliste: Anforderungen an die Software eines GMS, Teil 1

Entscheidungskriterium

In einem Gefahrenmanagementsystem (GMS) werden alle sicherheitsrelevanten Meldungen aus allen Gefahrenmeldeanlagen und sonstigen technischen Anlagen der zu schützenden Liegenschaften angezeigt und bearbeitet. Zusätzlich werden alle relevanten Meldungen im System erfasst und bearbeitet, die über andere Wege (z. B. über Telefon oder persönliche Ansprache) übermittelt werden.

Für ein GMS ist daher die Auswahl der passenden Software ein sehr wichtiges Entscheidungskriterium. Aus diesem Grund sollte darauf geachtet werden, dass das einzusetzende GMS mindestens folgende Leistungsmerkmale erfüllt:

Die folgend aufgeführten Funktionen sollten in jedem GMS unbedingt realisiert sein:

- Die Software (und auch die benötigte Hardware) muss über eine möglichst große Ausfallsicherheit verfügen. Ein redundanter Aufbau des Systems und eine Bearbeitung von Alarmen, Störungsmeldungen und sonstigen Informationen von einem anderen Standort aus muss möglich sein.

Ausfallsicherheit

- Das GMS muss, nach einem Neustart, eigenständig alle Informationen aus den angeschlossenen sicherheitstechnischen und sonstigen Subgewerken abfragen, damit sichergestellt ist, dass der aktuelle Zustand aller Anlagen und Melder angezeigt wird. Mit dem automatischen Wiederanlaufverfahren werden für die Anwendungen alle erforderlichen Zustände initialisiert.

Wiederanlaufverfahren

  Eine Ausnahme sollte bei einer Alarmübertragung gemäß VdS 2465 geprüft werden, da eine Abfrage der einzelnen Zustände über das Alarmübertragungsnetz sehr lange dauern kann. Dabei ist zu prüfen, ob die Alarmempfangseinrichtung derartige Anfragen automatisch ignoriert oder diese transparent an das Alarmübertragungsnetz weitergeleitet werden.

Ausnahme prüfen

- Sollte im GMS ein Lizenzmanagementsystem integriert sein, darf ein Defekt oder Ausfall der Lizenzverwaltung nicht zum Ausfall des GMS führen. Das heißt, die Lizenzverwaltung darf die Redundanz bzw. Ausfallsicherheit des GMS-Systems nicht beeinträchtigen. Die Lizenzverwaltung darf nur die Verwendung von nicht lizenzierter Hard- und Software unterbinden. Dazu ist die Lizenzverwaltung mindestens als fehlertolerantes System (Fail Operational) gemäß DIN EN 61508 zu realisieren.

Fehlertolerantes Lizenzmanagement

- Je angeschalteter Anlage bzw. angeschaltetem System muss es möglich sein, den aktuellen Funktions- und Meldungsstatus mit Hilfe von zusammenführenden Darstellungen anzuzeigen. Hierfür sind Ampeldarstellungen zu nutzen:

Ampeldarstellung pro System

  - grün leuchtend: Anlage fehlerfrei in Funktion, Melder in Betrieb und nicht ausgelöst
  - gelb blinkend: Anlage abgeschaltet, in Wartung bzw. Revision, Melder abgeschaltet, in Störung oder Revision
  - rot blinkend: Anlage ausgefallen bzw. gestört, Melder ausgelöst.

Eine vom Auftraggeber gewünschte individuelle Anpassung der Statusmeldungen muss möglich sein.

Alarm- und Meldungsliste

- Alle Alarme, Störungsmeldungen und sonstigen Informationen, die im GMS selbst oder in den angeschlossenen sicherheitstechnischen und sonstigen Subgewerken erzeugt werden, sind in einer Alarm- und Meldungsliste auf einer einheitlichen Bedienoberfläche des GMS immer in derselben Weise darzustellen.

» Anpassung der Statusmeldungen. «

Von jedem Arbeitsplatz aus

- Grundsätzlich müssen alle Alarme, Störungsmeldungen und sonstigen Informationen von allen Arbeitsplätzen aus bearbeitet werden können. Dazu sind die Alarme, Störungsmeldungen und sonstigen Informationen nach Prioritäten und nach dem Eintreffen der Meldungen geordnet in einer oder mehreren Alarm- und Meldungslisten anzuzeigen. Sollte es benötigt werden, müssen die Alarme, Störungsmeldungen und sonstigen Informationen bestimmten Arbeitsplätzen zugewiesen werden können. Diese Aufteilungen müssen alarmbezogen, nach Funktionen der Bearbeiter oder sonst wie vom Auftraggeber gewünscht aufgeteilt werden können. Z. B.:

  - alle Brandalarme zu Arbeitsplatz 1
  - alle anderen Alarme, Störungsmeldungen und sonstigen Informationen zu Arbeitsplatz 2
  - alle Alarme des Objektes 1 zu den Arbeitsplätzen 1 bis 3
  - alle Alarme des Objektes 2 zu Arbeitsplatz 4
  - alle Alarme der Objekte 3 bis 5 zu Arbeitsplatz 5
  - etc.

Sperrung von Vorfällen

- Werden ein Alarm, eine Störungsmeldung und eine sonstige Information von einem Bearbeiter aus der Alarm- und Meldungsliste ausgewählt, muss er für alle anderen Bearbeiter zur Auswahl gesperrt sein und der die Meldung bearbeitende Mitarbeiter ist anzuzeigen. Eine Übergabe eines in Bearbeitung befindlichen Alarms, einer Störungsmeldung und einer sonstigen Information zu einem anderen Arbeitsplatz bzw. Bearbeiter muss möglich sein.

Workflow-Routinen

- Für alle auftretenden Alarme, Störungsmeldungen und sonstigen Informationen sind in angemessener Weise vordefinierte Workflow-Routinen im GMS datentechnisch zu hinterlegen.

Verknüpfbare Systeme

- Automatische oder manuell herstellbare Verknüpfungen zwischen den an das GMS angeschlossenen Systemen (z. B. Brandmeldeanlagen, Einbruchmeldeanlagen, Kommunikationssysteme etc.) müssen erstellt werden können, um alle ereignisrelevanten Informationen darstellen und alle benötigten Kommunikationswege nutzen zu können.

BMA, EMA etc.

- Die im GMS benötigten Steuerungsmöglichkeiten (z. B.: Brandmeldeanlagen, Einbruchmeldeanlagen, Video, ausgewählte Türen, Tore, Schranken, Schleusen, Drehsperranlagen, Beleuchtungen, Lichtsignalanlagen und sonstigen benötigten Steuermöglichkeiten) sind über die an das GMS angeschlossenen Systeme und über direkte Ansteuerungen aus dem GMS heraus bereitzustellen.

Bewegtbild

- Das GMS muss in der Lage sein, Videobilder, die von einem Videomanagementsystem oder von dessen Bildaufzeichnungssystemen zur Verfügung gestellt werden, darzustellen und einfache Steuermöglichkeiten der Kameras zu ermöglichen. Z. B.:

- Steuerung von "Pan, Tilt & Zoom" (PTZ) Verfolgerkameras
- Zoom-Funktionen auf beliebige Ausschnitte von Videobildern
- etc.

- Mithilfe der automatisch oder manuell ausgewählten Visualisierung, der zur Verfügung gestellten Kommunikationstechnik und der dargestellten Handlungsanweisungen muss die vollständige Abarbeitung der anstehenden Alarme, Störungsmeldungen und sonstigen Informationen gewährleistet werden.
- Alle Aktionen im GMS sind personen-, alarm-, leitungs- und platzbezogen zu protokollieren und über Filterfunktionen auswählbar als Protokolldatei und für statistische Auswertungen geeignet fälschungssicher abzuspeichern. Die daraus entstehenden Dateien müssen an bestehende Protokollstrukturen anpassbar und, als Kopie, zur Weiterverarbeitung aus dem System entnehmbar sein. Dazu sind die im System erstellten Protokolle und Statistiken in einem fälschungssicheren Format abzuspeichern. Eine Weiterleitung der erstellten Informationen per E-Mail oder auf anderen Wegen ist zu realisieren.
- Die systemeigenen Alarme, Störungsmeldungen und sonstigen Informationen des GMS sind in die Alarm- und Meldungsliste des GMS zu integrieren.
- Das GMS sollte mindestens die Bedienung und Administration in deutscher und englischer Sprache ermöglichen. Bei Bedarf sollten weitere Sprachen zur Verfügung gestellt werden können.
- Das GMS muss intern („On-Premise“) über ein umfangreiches Hilfesystem verfügen, damit die Bearbeiter nicht schon an einzelnen Arbeitsschritten scheitern. Ein Hilfesystem, das für die Hilfedateien auf eine Cloud via Internet zugreifen muss, sollte nicht verwendet werden.
- Alle im GMS benötigten Daten (z. B. Grundrisse und Übersichtspläne, Erstellung und Pflege von angeschlossenen Anlagen und Meldern, Handlungsanweisungen etc.) müssen, wenn gewünscht, vom Personal des Auftraggebers an die aktuellen Gegebenheiten anpassbar sein.
- Die Möglichkeit der Verschlüsselung bzw. Entschlüsselung aller Steuerungs-, Alarm- und Statusmeldungen von und zu den angeschlossenen Komponenten, Arbeitsplätzen und Anlagen sollte gegeben sein. Die

zu speichernden Daten des GMS müssen ebenfalls verschlüsselt abgelegt werden können. Bei der Verschlüsselung der Daten und Übertragungen müssen mindestens das Verfahren AES (256 Bit) und beim Schlüsselaustausch mindestens das Verfahren TLS 1.2 eingesetzt werden.

Anpassbare GUI

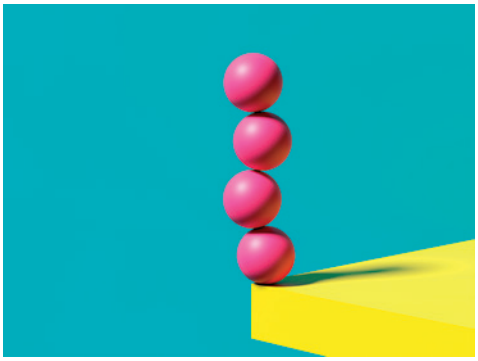
- Die Bildschirmoberflächen (Graphical User Interfaces, GUI) müssen an die Bedürfnisse der Benutzer angepasst werden können (z. B. Aufteilung der Fenster auf der Bildschirmoberfläche, Größe der Schrift und Darstellungen etc.). Dabei ist zu beachten, dass die Alarmlisten immer sichtbar sein müssen.

Management von Updates

- Bei Software-Updates zur Fehlerbereinigung und -verbesserung und Software-Upgrades zur Erweiterung des Funktionsumfangs müssen die vorhandenen Daten vollständig erhalten bleiben bzw. im Rahmen des Updates bzw. Upgrades automatisch angepasst werden. Die Software-Clients müssen sich bei Updates bzw. Upgrades automatisch bei der Anmeldung am Server aktualisieren.

Mindestens acht Nutzerrollen

- Jeder Arbeitsplatz und jeder Benutzer muss mit differenzierten Zugriffsrechten und Nutzungsmöglichkeiten versehen werden können. Diese Konfiguration erfolgt grundsätzlich durch den Systemadministrator des Auftraggebers. Es müssen mindestens acht verschiedene Berechtigungsebenen bzw. Benutzerrollen vorhanden sein: Administrator, Systembetreuer bzw. Datenpfleger, Standardnutzer, zwei Springer, Administrator und Systembetreuer des Wartungsunternehmens und einen Account als Reserve. Zusätzlich muss die Vergabe von rollenspezifischen Berechtigungen möglich sein.



Fälschungssichere Verschlüsselung

- Jede im GMS vorgenommene Aktion (z. B. Alarmierungen, Anwendereingaben und alle Bearbeitungsvorgänge) muss zur Gewährleistung einer Gerichtsverwertbarkeit unveränderbar und verschlüsselt dokumentiert und gespeichert werden können.

Integrierbarkeit analoger Meldungen

- Es muss im GMS die Möglichkeit geben, Meldungen, die nicht über die angeschlossenen Gefahrenmeldeanlagen übertragen werden, in das GMS aufzunehmen (z. B. Meldungen über Telefon). Für den manuellen Eintrag ist im GMS ein Stichwortverzeichnis zu integrieren, womit der Bearbeiter die versorgten manuellen Meldungen (z. B. Bombenalarm per Telefon) auswählen kann. Nach der Auswahl über das Stichwort erhält der Bearbeiter die passende Handlungsanweisung und kann den Alarm, analog zu den technischen Alarmen, bearbeiten.

Nachdem wir uns hier mit den grundsätzlichen Leistungsanforderungen an GMS-Software beschäftigt haben, folgt in Ausgabe 17 des Sicherheits-Berater Teil 2 mit einer Betrachtung der erforderlichen Funktionalitäten.

Der Autor Klaus Kirchhöfer
Bachelor of Business Administration Business Security (BBA)

Sicherheitsberater, Redaktionsmitglied des Sicherheits-Berater (seit 2000) mit den Spezialgebieten Sicherheitszentralen, Einsatzleitstellen, Kommunikation, Information Security Management (ISO 27001 Lead-Auditor)

CROWDSTRIKE

Kleingedrucktes in Großbuchstaben: Wer lesen kann …

Softwareupdate

… ist klar im Vorteil. Frischester Beleg für diese lebensnahe Wahrheit ist der globale „Cybervorfall" am 19.7.2024: CrowdStrike verteilte global ein Softwareupdate, das Millionen von Windows-Rechnern zum Absturz brachte. Wirklich unangenehm an der fehlerhaften Software war und ist, dass sie vor Ort, am PC des Geschehens, deaktiviert und entfernt werden muss. Damit dürfte der finanzielle Schaden, der durch den Ausfall der Rechner verursacht wurde, vom finanziellen Aufwand, der für die Behebung des Schadens nötig ist, vielleicht sogar übertroffen werden.

Finanzieller Schaden

Mehr als finanziellen Schaden muss man aber auch nicht befürchten, denn in weiser Einschätzung der eigenen Fähigkeiten hat CrowdStrike in seinen Geschäftsbedingungen (www.crowdstrike.com/terms-and-conditions-de) auch einen Vorbehalt eingebaut, der Seinesgleichen sucht:

Geschäftsbedingungen

ES GIBT KEINE GEWÄHRLEISTUNG, DASS DIE ANGEBOTE ODER CROWDSTRIKE-TOOLS FEHLERFREI SIND ODER DASS SIE OHNE UNTERBRECHUNG FUNKTIONIEREN ODER BESTIMMTE ZWECKE ODER BEDÜRFNISSE DES KUNDEN ERFÜLLEN. DIE CROWDSTRIKE-ANGEBOTE UND CROWDSTRIKE-TOOLS SIND NICHT FEHLERTOLERANT UND NICHT FÜR DEN EINSATZ IN GEFÄHRLICHEN UMGEBUNGEN AUSGELEGT ODER VORGESEHEN, DIE EINE AUSFALLSICHERE LEISTUNG ODER EINEN AUSFALLSICHEREN BETRIEB ERFORDERN. WEDER DIE ANGEBOTE NOCH DIE CROWDSTRIKE-TOOLS SIND FÜR DEN BETRIEB VON FLUGZEUGNAVIGATION, NUKLEARANLAGEN, KOMMUNIKATIONSSYSTEMEN, WAFFENSYSTEMEN, DIREKTEN ODER INDIREKTEN LEBENSERHALTENDEN SYSTEMEN, FLUGVERKEHRSKONTROLLE ODER ANWENDUNGEN ODER ANLAGEN BESTIMMT, BEI DENEN EIN AUSFALL ZU TOD, SCHWEREN KÖRPERVERLETZUNGEN ODER SACHSCHÄDEN FÜHREN KÖNNTE.

»Das ist einmal eine Ansage!«

Verantwortung des Kunden

Der Kunde stimmt zu, dass es in der Verantwortung des Kunden liegt, die sichere Nutzung eines CrowdStrike-Angebots und der CrowdStrike-Tools in solchen Anwendungen und Installationen zu gewährleisten.

Stirnrunzeln bei den Mitarbeitern?

Das ist einmal eine Ansage! Wenn der Anbieter sich im Klaren ist, dass seine Software vor allem Umsatz bringen soll, eigene Fehler üble Folgen haben und damit teuer werden könnten, dann ist er gewiss von seinen Juristen gut beraten, jegliche Haftung möglichst weit von sich zu schieben. Ob den Kunden dieses Unternehmens dieser Passus gegenwärtig war, ist dem Sicherheits-Berater nicht bekannt. Da CrowdStrike-Software aber vor allem in großen Unternehmen eingesetzt wird, ist durchaus die Frage erlaubt, ob diese Geschäftsbedingungen in die Nähe von juristisch bewanderten Mitarbeitern gelangt sind und deren Stirnrunzeln Beachtung fand.

Nicht bei kritischen Prozessen

Der geradezu demütige Hinweis in den AGB lässt sich aber spätestens jetzt so auslegen, dass die Crowdstrike-Produkte in KRITIS-regulierten Unternehmen (und in näherer Zukunft auch in allen Unternehmen, die nach NIS-2 und DORA-Regeln agieren) höchstens auf Rechnern weit abseits der kritischen Prozesse und Leistungen genutzt werden dürfen.

Sicherheitssoftware ad absurdum

Auf kritischer IT wäre der Einsatz nur dann zu verantworten, wenn vor dem produktiven Einsatz ein ausführlicher Test in einer aussagefähigen Testumgebung durchgeführt würde. Das allerdings würde den Einsatz einer Sicherheitssoftware, die verspricht, auch ganz aktuelle Erkenntnisse aus der Analyse neuer Schwachstellen und Vorfälle zur Erkennung und Eindämmung von sicherheitsrelevanten Ereignissen zu nutzen, ein wenig ad absurdum führen.

Qualitätssicherung empfohlen

Da der Sicherheits-Berater stets bemüht ist, konstruktiv zu sein, sei noch ein Hinweis an CrowdStrike erlaubt. Dort wirbt man mit der Selbstauskunft:

„Bei CrowdStrike ist KI mehr als eine Funktion – sie steckt in unserer DNA. Mit Modellen, die täglich mit Billionen von Datenpunkten trainiert werden, können wir Bedrohungen vorhersagen und stoppen."

Es sollte heutzutage KI-Modelle geben, die mit guter Trefferquote Anfängerfehler in Programmquellen finden. Folgt Eurer DNA und lasst Eure KI NULL-Pointer in C++ Programmquellen vorhersagen. Oder anders ausgedrückt: Noch besser wäre es, wenn ein kundiges Team in Eurem Hause sich mit Qualitätssicherung befasste!

Der Autor Werner Metterhausen
Diplom-Informatiker

Sicherheitsberater, Redaktionsmitglied des Sicherheits-Berater (seit 1997) mit den Spezialgebieten RZ-Zertifizierung, Datenschutz, Informationssicherheit (ISO 27001 Lead-Auditor)

DATENSCHUTZ

Berechtigtes Interesse: eigene Meinung vs. Meinung anderer

Letztes Mittel

Das „berechtigte Interesse" ist eine von mehreren Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im Rahmen der Datenschutz-Grundverordnung (DSGVO). Es wird häufig als letztes Mittel herangezogen, wenn die anderen Rechtsgrundlagen nicht greifen oder weil eine eingehende Auseinandersetzung mit der Rechtsverordnung zu

umständlich erscheint. Vielen Verantwortlichen ist nicht bewusst, dass es nicht ausreicht, das eigene Interesse zu bekunden, sondern dass es einer Prüfung und bestenfalls einer Dokumentation bedarf.

Berechtigtes Interesse

Klären wir zunächst, was ein „berechtigtes Interesse" ist. Der Begriff ist flexibel auslegbar und umfasst somit jedes rechtliche, tatsächliche, ideelle oder wirtschaftliche Interesse. Nach Auffassung der Europäischen Kommission (commission.euopa.eu, Kurzlink https://tinyurl.com/8ncmt725) kann ein "berechtigtes Interesse" an der Verarbeitung personenbezogener Daten vorliegen, wenn "Sie personenbezogene Daten verarbeiten müssen, um Aufgaben im Zusammenhang mit Ihrer Geschäftstätigkeit zu erfüllen."

Eingeschränktes Interesse

Das Wort „berechtigt" schränkt das Interesse dahingehend ein, dass das verfolgte Interesse nicht gegen Rechtsvorschriften verstoßen oder einem strafrechtlichen oder sonstigen Verbot unterliegen darf. In den Erwägungsgründen der DSGVO wird ausgeführt, dass folgende Zwecke ein berechtigtes Interesse darstellen können:

- Direktmarketing, Kundenakquise, Teilnahme am Wirtschaftsverkehr
- bestehende Geschäftsbeziehung
- Verhinderung von Betrug
- Ausübung des Rechts auf Meinungsfreiheit

Verantwortliche, die ihre personenbezogene Datenverarbeitung auf das berechtigte Interesse (nach Art. 6 Abs. 1 lit. f DSGVO) stützen möchten, sollten wissen, dass für die Anwendung dieser Rechtsgrundlage drei Voraussetzungen – kumulativ – erfüllt sein müssen und was die Datenverarbeitung eigentlich umfasst. Dies lässt sich anhand einer dreiteiligen Fragestellung überprüfen:

1. Zweckerfüllung

Rechtmäßig, fair und vertretbar?

Ist die Verarbeitung rechtmäßig, fair und vertretbar? Die Antwort auf diese Frage sollte weder vage noch zu weit gefasst sein und angeben, zu Gunsten welcher Partei das Interesse überwiegt.

2. Erforderlichkeit

Ein Muss für die Zielerreichung?

Folgende Fragen können bei der Erforderlichkeitsprüfung helfen: Muss ich diese personenbezogenen Daten verarbeiten, um mein Ziel zu erreichen? Kann ich mein Ziel auch

mit weniger Daten erreichen? Hier wird der Ansatz verfolgt, zu prüfen, ob ein anderes, milderes Mittel den Zweck erreichen kann, um nicht übermäßig in die Privatsphäre der Betroffenen einzugreifen. Auch die Möglichkeit, weniger Daten zu verarbeiten, stellt ein milderes Mittel dar. Es ist schwierig, sich auf ein berechtigtes Interesse als Grundlage für die Datenverarbeitung zu berufen, wenn es effektive Alternativen gibt.

3. Abwägung

Nachvollziehbarkeit

Als nächstes sind die Interessen der Betroffenen, einschließlich ihrer Grundrechte und Grundfreiheiten, gegen die eigenen Interessen abzuwägen, was zunächst eine sorgfältige Gegenüberstellung und Priorisierung voraussetzt. Es liegt auf der Hand, dass der für die Verarbeitung Verantwortliche seine Interessen wesentlich höher gewichtet als die Interessen Dritter. Die Abwägung ist schwierig, aufwendig und sollte nicht auf einer subjektiven Meinung beruhen, sondern nachvollziehbar sein und zeigen, dass mögliche Einwände berücksichtigt wurden.

» Kann ich mein Ziel auch mit weniger Daten erreichen? «

Beispiele für die Interessen betroffener Personen sind nach der Charta der Grundrechte der Europäischen Union:

- Recht auf Privatsphäre (Art. 7)
- Schutz/Sicherheit der personenbezogenen Daten (Art. 8)

Gewichtung

Dagegen ist das Interesse des Verantwortlichen schwerer zu gewichten, wenn beispielsweise die Verarbeitung nicht nur ihm, sondern auch der Allgemeinheit zugutekommt. Weitere Kriterien, die bei der Gewichtung berücksichtigt werden können, sind z. B. die Art der Daten, die Datenmenge, die Datenquellen, die Dauer und die Sicherheit der Verarbeitung.

Vernünftige Erwartungen

Zusätzlich verlangt der Erwägungsgrund 47 DSGVO die Berücksichtigung der vernünftigen Erwartungen betroffener Personen. Es ist also zu prüfen, ob die betroffenen Personen zum Zeitpunkt der Erhebung ihrer Daten und unter Berücksichtigung der Umstände, unter denen die Daten erhoben werden, vernünftigerweise vorhersehen können, dass diese Daten möglicherweise für den beabsichtigten Zweck verarbeitet werden.

Stellschrauben fürs Eigeninteresse

Leider gibt es keine objektiven Kriterien, die als Maßstab für die Interessenabwägung herangezogen werden könnten. Bei Zweifeln oder beim Überwiegen der Betroffeneninteressen sollte die Umsetzung der DSGVO-Grundsätze bei den eigenen Verarbeitungsprozessen betrachtet werden. Stellschrauben, mit denen das Eigeninteresse stärker gewichtet werden kann, sind z. B. die Erhöhung der Sicherheit der Datenverarbeitung, die Reduzierung der Datenmenge oder auch die Anzahl der Auftragsverarbeiter, die diese Daten für den Verantwortlichen verarbeiten sollen.

Recht auf Widerspruch

Die Einschätzung, dass die Verarbeitung nicht unverhältnismäßig ist, sollte dokumentiert und ggf. in der Datenschutzinformation erläutert werden. Betroffenen bleibt die Möglichkeit der Verarbeitung, die auf einer Interessensabwägung beruht, zu widersprechen. Das Recht auf Widerspruch ist jedoch nicht absolut.

Ausnahmeregel

Lässt sich anhand der dokumentierten Interessenabwägung nachweisen, dass das eigene Interesse an der Weiterverarbeitung das Widerspruchsrecht der betroffenen Person überwiegt, besteht die Chance, die Verarbeitung fortsetzen zu können. Dies gilt jedoch nicht für das Direktmarketing auf der Grundlage des legitimen Interesses. Hier muss die Verarbeitung nach einem Widerspruch unterbleiben.

::: Cornelia Last :::

SICHERHEITSPLANUNG

NIS-2: kritische Infrastrukturen im Fokus

Digitale Angriffe

Wie täglich den Medien zu entnehmen und von dem einen oder anderen Betroffenen im Unternehmen bereits hautnah miterlebt, ist durch die globale Vernetzung in unserer digitalen Welt ein nicht zu unterschätzendes Risiko entstanden. Cyberangriffe sind so alltäglich geworden wie Ladendiebstähle. Waren es vor einiger Zeit nur einzelne Unternehmen oder auch nur Abteilungen, so weiten sich die digitalen Angriffe auch auf die so genannten kritischen Infrastrukturen aus.

Schutz kritischer Infrastruktur

Bei dem gerade beschriebenen Szenario handelt es sich um ein internationales Problem, auf das EU-seitig durch die Verabschiedung des NIS-2-Gesetzes reagiert wurde. NIS-2 steht für die „zweite EU -Richtlinie zur Netzwerk- und Informationssicherheit". Das Gesetz soll bewirken, dass Betreiber solcher kritischen Infrastrukturen – also Kraftwerke, Wasserversorger, Krankenhäuser etc. – ihre Netze sicherer machen. Eine zentrale Vorgabe von NIS-2 betrifft die Implementierung eines Risiko-Managementsystems. Da es bisher keine verbindlichen Vorgaben oder Vorschriften für die Nutzung eines bestimmten Standards eines Informationssicherheits-Managements (ISMS) gibt, kann jeder Betreiber ein geeignetes Vorgehen wählen. Hierzu stehen bereits nationale und internationale Normen und Standards zur Verfügung, die als Best Practice für den Aufbau eines ISMS verwendet werden können. Dazu zählen unter anderem:

- BSI IT-Grundschutz
- BSI KRITIS-Standard und
- DIN ISO 27001

Physischer Schutz erforderlich

In einigen der oben genannten Dokumente ist auch die Rede von physischer Absicherung kritischer Unternehmen. Dabei spannt sich der Bogen von der Beschränkung von

Zugriffen Unberechtigter auf kritische Netzwerkstrukturen bis hin zur Abwehr von Angriffen oder die Vermeidung von Sabotage. Aber auch die Gefahren ausgehend vom Umfeld der Liegenschaft oder den Umweltbedingungen sind zu betrachten. All diese möglichen Risiken bergen Gefahren für die Betriebssicherheit kritischer Infrastrukturen. Es ist im Grunde genommen egal, ob ein Schaden durch einen Cyberangriff, durch eine Vor-Ort-Sabotage oder durch ein Naturereignis, wie zum Beispiel Starkregen, eintritt. In allen Fällen kann dabei die Betriebssicherheit negativ beeinflusst werden.

» Da wäre als erstes die Identifizierung von Bedrohungen. «

Konzeptioneller Ansatz

Um sich als Betroffener, also Betreiber einer kritischen Infrastruktur, ein Bild von der Bedrohungssituation zu machen, hilft es wenig, sich bei den vereinzelten Vorgaben und Anforderungen aus den oben erwähnten Normen und Richtlinien zu bedienen. Man muss hier konzeptionell unter Berücksichtigung der jeweiligen Situation und der speziellen Anforderungen herangehen, was nur durch eine klassische Sicherheitskonzeption vollumfänglich geschehen kann.

Risikoanalyse

Da wäre als erstes die Identifizierung von Bedrohungen. Man spricht hier von der Durchführung einer Risikoanalyse, die sämtliche potenziellen Risiken berücksichtigt, die Auswirkungen auf die sichere Betriebsweise der jeweiligen Einrichtung haben können. Das ist nicht nur der mögliche Eindringtäter, der Böses im Schilde führt, sondern auch ein Innentäter mit Sabotageabsichten. Auch die oben bereits erwähnten Gefährdungen durch die Umwelt, wie beispielsweise Starkregen, sind zu berücksichtigen. Dabei kann es beispielsweise zu Überschwemmungen und somit Wassereintritt in Räume mit kritischen Infrastrukturen, z. B. Trafo, Elektrounterverteilungen, Tanklager von Netzersatzanlagen, kommen. So etwas bei ungünstiger topographischer Lage kann eben auch zum Beispiel einem Krankenhaus den Garaus machen.

Schutzzieldefinition

Hat man alle Risiken erfasst und in ihrer Kritikalität eingestuft, geht man dazu über, aus diesen Risiken Schutzziele abzuleiten, um erstere zu minimieren. Bleiben wir bei den oben genannten Beispielen und betrachten den unberechtigten Zutritt in einen Sicherungsbereich, dann folgt daraus das Schutzziel: „Vermeidung eines unberechtigten Zugangs zur Abteilung xy". Ein weiteres Schutzziel wäre: „Vermeidung von Wassereintritt in kritische Versorgungsräume" resultiert aus dem potenziellen Risiko des Wassereintritts bei Starkregen. Die nun definierten Schutzziele bilden den Anforderungskatalog für alle zu ergreifenden Maßnahmen, die zur Erfüllung der Schutzziele dienen.

Schutzmaßnahmen

Um das Schutzziel erreichen zu können, müssen Maßnahmen ergriffen werden. Es existiert eine Vielzahl von Maßnahmen, die zur Erfüllung des einen Schutzzieles führen können. Greifen wir beispielsweise das Schutzziel „Vermeidung eines unberechtigten Zugangs in Abteilung xy" wieder auf, so kann das mit folgenden Maßnahmen erreicht werden:

- Vereinzelungsanlage
- Personenschleuse
- Zugangskontrolle mittels Kartenleser, PIN und biometrischer Erkennung
- Zugangskontrolle mittels Kartenleser und PIN
- Zugangskontrolle mittels Kartenleser
- Zugangskontrolle mittels Schlüssel

Produktneutrale Beratung

Um dann eine der Maßnahmen für den konkreten Anwendungsfall auszuwählen, bedarf es weiterer Einschränkungen und Bedarfsermittlungen, weil nicht nur sehr unterschiedliche Preisschilder an den Maßnahmen hängen, sondern auch weil bauliche und organisatorische Umstände und vor allem der jeweilige Sicherheitsanspruch die eine oder andere Maßnahmen nicht zulassen. Empfehlungen oder Vorschläge von Lösungsansätzen und konkreten Maßnahmen innerhalb einer Sicherheitskonzeption sollten produktneutral sein und sich nach Erreichen des jeweiligen Schutzziels orientieren. Dabei gibt es nicht nur die „eine" Lösung, sondern eine Vielzahl an Möglichkeiten. Die von den Herstellern häufig suggerierte Vorstellung, dass gerade ihr Produkt für diesen Anwendungsfall genau das richtige ist, hat eher eine Erhöhung des Umsatzes statt der Sicherheit zum Ziel. In vielen Projekten sind die Produkte bereits in den Köpfen der Verantwortlichen, wo sie schwer wieder herauszubekommen sind. An dieser Stelle ist ein hohes Maß an Beratung notwendig.

» Es bedarf weiterer Einschränkungen und Bedarfsermittlungen. «

Im Umkehrschluss kann man auch mit nur einer Maßnahme mehrerer Schutzziele abdecken, zum Beispiel der Einsatz von Videokameras zur:

1. Überwachung
2. Verifizierung
3. und Detektion von Eindringversuchen.

Struktur und Konzeption

Letztendlich ist eine strukturierte und konzeptionelle Vorgehensweise wie oben beschrieben zwingend notwendig, um gemeinsam mit dem Kunden ein stabiles Sicherheitskonzept auf die Beine zu stellen. Ein wichtiger Faktor dabei, wie auch in der anschließenden Planungs- und Umsetzungsphase, ist die Berücksichtigung und Einhaltung der Gesetze und geltenden Normen und Richtlinien.

Der Autor Peter Schmidt
Diplom-Ingenieur (FH)

Sicherheitsberater, Redaktionsmitglied des Sicherheits-Berater (seit 2000) mit den Spezialgebieten Sicherheitstechnik und Klimatisierung von Rechenzentren

SICHERHEITSMANAGEMENT

Was ist eigentlich der Handbereich?

Definitionsbedarf

Ein Begriff wie „Handbereich" geht uns üblicherweise sehr schnell über die Lippen: Sätze wie *„Innerhalb des Handbereichs muss eine Fassade einen besonderen Schutz aufweisen."* oder *„Außerhalb des Handbereichs können Überwachungsmaßnahmen reduziert werden."* lesen sich in vielen Sicherheitskonzepten. Was man mit dem Begriff Handbereich aber konkret meint, überlässt man mit einer bewussten oder auch unbewussten Unschärfe der Formulierung oft dem Leser. Das ist nicht immer gut, daher haben wir uns mit dem Begriff einmal auseinandergesetzt.

Selbsttest

Funktional gesehen geht es um den Bereich, in dem durch Personen von außen ohne weitere Hilfsmittel auf die Fassade eines Gebäudes eingewirkt werden kann. Recht zweifelsfrei geht es also am Boden los und erstreckt sich über die gesamte Breite einer Außenfront bis zu – und das ist die eigentlich zu diskutierende Größe – einer bestimmten Höhe an der Fassade. Nun kann jeder einmal selbst den Test machen und ausprobieren, wie hoch er ohne Hilfsmittel greifen kann. Dem Autor dieses Beitrages gelingt es beispielsweise, mit 178 Zentimetern Körpergröße bis etwa 2,30 Meter hochzureichen, wobei im oberen Bereich ein Manipulieren von Fassadenelementen nicht mehr möglich wäre. Mit einfachen Hilfsmitteln wie beispielsweise Trittstufen lässt sich jedoch ein etwas erhöhter Bereich erschließen. Wo sollte man aber jetzt hier die Grenze ziehen?

Bei solchen Fällen gibt es immer den Reflex, nach dem Stand der Technik zu suchen, den Normen, Vorschriften oder Richtlinien repräsentieren. Bei einer entsprechenden Recherche stellt man fest, dass der Begriff Handbereich erst einmal sehr stark durch die Elektrosicherheit besetzt ist. In diesem Segment geht es aber darum, das Berühren gefährlicher aktiver Teile möglichst wirksam zu verhindern und somit Gefährdungen für Personen entgegenzuwirken. Konkret ist in der DGUV-Information 203-002 nämlich beschrieben, dass der Handbereich als Reichweite eines Menschen von der Standfläche aus gemessen

- nach oben mindestens 2,5 Meter
- in seitlicher Richtung sowie nach unten mindestens 1,25 Meter

beträgt. Wir erkennen aber schnell, dass hier nicht die Frage beantwortet wird, die wir gestellt haben, nämlich den Handbereich für eine Sicherheitskonzeption zu ermitteln. Vielmehr stellt man sich hier eine Plattform in einer Schalt- oder Industrieanlage vor, die für Instandhaltungstätigkeiten installiert ist und von elektrisch aktiven Teilen umgeben ist. Genau für einen solchen Fall sind die genannten Maße einzuhalten – für unsere Frage aber sind sie nicht relevant.

»Klarheit beugt an dieser Stelle Missverständnissen vor.«

Vielmehr finden wir in mehreren Publikationen der VdS Schadenverhütung GmbH klare und sogar noch gleichlautende Aussagen. Zum Beispiel ist in der VdS-Richtlinie 2311, Planung und Einbau von Einbruchmeldeanlagen, definiert, dass der Handbereich der Bereich ist „der sich bis 3 Meter oberhalb einer frei zugänglichen Fläche befindet". Gleichwohl verwundert es etwas, dass offenbar keine DIN- oder EN-Norm den Begriff aufgreift und eine entsprechende Aussage dazu trifft.

Da wir also in anderen Regelwerken keine entsprechenden Zahlen finden und die von uns überprüften VdS-Richtlinien alle mit einer gleichlautenden Formulierung daherkommen, können wir für den Moment bis auf Weiteres davon ausgehen, dass für die Festlegung des Handbereichs die Obergrenze von drei Metern eine praxistaugliche und belastbare Größenordnung darstellt. Oberhalb dieser Höhenmarke kann angenommen werden, dass Manipulationen an der Fassade nur mit aufwendigen Hilfsmitteln wie entsprechend großen Leitern, Hebebühnen oder Hubsteigern möglich sind. Je nachdem wie Risiken und Schutzziele definiert wurden, kann man also oberhalb von drei Metern anders vorgehen als darunter, oder eben je nach Objekt und Schutzbedarf auch nicht.

Letztlich ist es immer dem Autor einer Sicherheitskonzeption überlassen, welchen Bereich er für sein individuelles Vorhaben als Handbereich annimmt. Er sollte ihn aber klar

benennen, beispielsweise für die Fassadenelemente bis einschließlich des ersten Obergeschosses Schutzmaßnahmen gegen direktes Manipulieren fordern, oder eben bis zu einer Höhenmarke von drei Metern oberhalb der Geländegrenze. Andere Sicherheitskonzepte betrachten eine Fassade nicht differenziert nach Höhe und machen gleichwertige Maßnahmen über die gesamte Höhe verpflichtend. Klarheit beugt an dieser Stelle Missverständnissen vor, die die Wirksamkeit einer Sicherheitskonzeption beeinträchtigen könnten.

Eindeutige Benennung

Der Autor Jörg Schulz
Bachelor of Business Administration Business Security (BBA)

Sicherheitsberater, Redaktionsmitglied des Sicherheits-Berater (seit 2003) mit dem Spezialgebiet Videoüberwachung, Zutrittskontrolle, Gefahrenmeldetechnik, Sicherheitszentralen, Hochverfügbarkeit von RZ-Infrastrukturen

VERKEHRSSICHERHEIT

VZM-Gruppe nimmt an ADAC-Fahrsicherheitstraining teil

Am 29.6.2024 trafen sich Mitarbeiter der VZM GmbH und der SIMEDIA-Akademie in Weilerswist auf dem Gelände des ADAC, um ihr privates oder dienstliches Fahrzeug besser kennenzulernen.

Bildquelle:
Alice Hoffmann/VZM GmbH

Insgesamt 16 Mitarbeiter wollten es genauer wissen. Das Unternehmen spendierte das Training, die Getränke und ein gemeinsames Mittagessen. Für das leibliche Wohl war also gesorgt.

Für interessierte Unternehmen ist wissenswert, dass das Training für die Beschäftigten von der Verwaltungs-Berufsgenossenschaft unterstützt wird. Jeder Teilnehmer erhält einen Gutschein von insgesamt 75 Euro, der von den Gesamtkosten beim ADAC direkt abgezogen wird. Daher ist es wichtig, das Training vorab zu beantragen und die Voraussetzungen der VBG zu beachten, alle Infos dazu: www.vbg.de/cms/arbeitsschutz/arbeit-gestalten/versicherssicherheit/fahrtrainings.

ABS, ESP und TCS

Unsere Teams starteten zu je acht Personen. Der jeweilige Trainer für den Tag stellte eingangs Fahrsicherheitsfeatures vor, die neuere Fahrzeuge bereits mitbringen. So wurde kurz das Antiblockiersystem (ABS), das Elektronische Stabilitätsprogramm (ESP) oder das Traktionskontrollsystem (TCS) erläutert und gleichzeitig festgestellt, wer mit welchem Pkw an den Start ging. Die Reifenwahl ist ebenfalls entscheidend für so manche Reaktion, doch dazu später mehr. Der Trainer notierte sich also auch, mit welchem Reifen das jeweilige Fahrzeug unterwegs war.

Beeindruckende Vollbremsungen

Zuerst galt es, die nötigen Einstellungen vorzunehmen oder zu überprüfen. Sind die Spiegel optimal ausgerichtet, sitzt man richtig, also aufrecht und natürlich vor allem: ist man angeschnallt? Nachdem das sichergestellt war, bestand die erste Übung darin, durch Bremsen vor einem Pylonen beziehungsweise Verkehrsleitkegel zum Stehen zu kom-

men. Das war bereits beeindruckend – „aber da geht noch viel mehr", so das Trainerteam. Während des gesamten Tages war man über Walkie-Talkie mit den Trainern verbunden und wurde immer wieder mit Tipps und Tricks versorgt. Wenn man dachte, „das war jetzt eine Vollbremsung", hatte man in den meisten Fällen doch noch nicht alles gegeben. Deshalb ging es wieder und immer wieder in neue Bremsmanöver. Zum Ende hatten die Teilnehmer hautnah erfahren, dass beherztes Bremsen das A und O in brenzligen Situationen sein kann.

Ein Stoß gegen die Hinterachse

Doch Steigerungen sind immer möglich, so auch hier. Die Fahrbahn wurde geflutet und so zur Aquaplaningstrecke umgestaltet, in der plötzliche Hindernisse auftraten. Als nächste Stufe galt es auf der gleichen Strecke noch weitere Anforderungen zu meistern. So bekam man beispielsweise zu Beginn der Bahn in die eine oder andere Richtung einen kurzen Impuls, den es auszugleichen galt. Also Regen, nasse Fahrbahn, einen Stoß gegen die Hinterachse, Hindernisse – was will man mehr? Anlass zur Sorge bestand allerdings nie. Jeder trainierte nur so viel er wollte und die Geschwindigkeit, mit der die Übungen durchfahren wurden, konnte stets individuell angepasst werden.

Empfehlen das Fahrsicherheitstraining weiter: die Teilnehmer der VZM-Gruppe
Bildquelle: Alice Hoffmann/VZM GmbH

Gelungene Drift-Einlagen

Jetzt ging es in den „Ring". Hier konnten die Teilnehmer das Verhalten in Kurven mit ihren Fahrzeugen unter verschiedenen Bedingungen ausprobieren. Dazu gehörte auch, im Kreisel das ESP auszuschalten. Da traten bei vielen Kollegen schon einige recht gelungene Drift-Einlagen der Teilnehmer beobachtet werden.

Lerngewinne in der Zusammenfassung:

Lohnendes Sicherheitstraining

1. Je höher die Geschwindigkeit, desto weniger ist im echten Gefahrenfall vom Gelernten umsetzbar.

2. Im Herbst oder Winter mit Sommer- statt Winterreifen unterwegs zu sein, macht aus einer grundsätzlich beherrschbaren Situation ein No-Go.

3. Die Teilnahme am Sicherheitstraining hat sich gelohnt. Die gewonnene praktische Erfahrung und das vermittelte Wissen können im Notfall – der hoffentlich nicht eintrifft – wahrscheinlich dabei helfen, richtig zu handeln. Eine Auffrischung des Trainings ist daher schon in der Planung.

Die Autorin Manuela Wagner

Büroleiterin sowie Beauftragte für Qualitätsmanagement und Brandschutz (beides bei der VZM GmbH, Bonn)

Nachrichten

Wirkungsmechanismen von Protestaktionen. Das Online-Kurzseminar der SIMEDIA Akademie „Bedrohung durch Protestaktionen: Eine Herausforderung für die Unternehmenssicherheit" am 5. September 2024 beleuchtet die Wirkungsmechanismen von Protestaktionen, beschreibt „Angriffsflächen" in einer 360 Grad-Perspektive und zeigt Handlungsoptionen auf. Denn öffentlichkeitswirksame Aktionen, Proteste, Sitzstreiks, Besetzungen: Aktivisten richten sich längst nicht mehr nur gegen Unternehmen selbst, auch ihre Repräsentanten geraten zunehmend in den Fokus. simedia.de

Zukunftssichere Rechenzentren. Das neue Online-Seminar der SIMEDIA Akademie „Zukunftssichere Rechenzentren – Innovation und Effizienz im Fokus" am 28. Oktober 2024 bietet eine Plattform, um sich über Innovationen und Trends zu informieren. Die Veranstaltung fokussiert auf die Themen Zukunft der Kühlung von Rechenzentren, Energieeffizienzgesetz: Anforderungen und Chancen, aktuelle Entwicklungen der technischen Infrastruktur, Normen versus Innovation sowie Bezug auf das KRITIS-Dachgesetz. Schließlich sieht sich das Management von Rechenzentren mit neuen Herausforderungen und Chancen konfrontiert: Energieeffizienz, innovative Kühltechnologien und strenge Sicherheitsvorgaben. rechenzentrum.simedia.de

Folgemaßnahmen des BSI nach Crowdstrike-Vorfall. Nach den weltweiten IT-Störungen am 19. Juli 2024 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Gespräch mit den Software-Unternehmen Crowdstrike und Microsoft erste Maßnahmen entwickelt, um vergleichbare Vorfälle künftig zu vermeiden. Das BSI will nach eigener Aussage in Gesprächen mit Microsoft, Crowdstrike und Herstellern vergleichbarer Softwarelösungen darauf hinwirken, dass das jeweilige Betriebssystem auch bei schwerwiegenden Fehlern immer mindestens in einem abgesicherten Modus gestartet werden kann. bsi.bund.de
Kurzlink tinyurl.com/34u2m3u4

it-sa Expo&Congress. Trends & Innovationen der IT-Securitybranche stehen bei der diesjährigen it-sa vom 22. bis 24. Oktober 2024 auf dem Gelände der NürnbergMesse im Fokus. itsa365.de

Höchster Anstieg globaler Cyberattacken in den letzten zwei Jahren. Check Point Research hat neue Daten zu Cyberangriffstrends veröffentlicht, die einen Anstieg der Angriffe von 30 Prozent im zweiten Quartal 2024 aufzeigen. checkpoint.com
Kurzlink tinyurl.com/bx2wzs7f

Lünendonk®-Liste 2024 „Führende Sicherheitsdienstleister". Laut einer aktuellen Lünendonk®-Liste verzeichneten die Top 25 der Umfrageteilnehmer im Jahr 2023 ein Umsatzwachstum von ca. 7,9 Prozent. Die Top 10 steigerten ihren Umsatz demnach sogar um 12,6 Prozent. Dagegen sinkt die Zahl der Beschäftigten bei den Top 25 im Durchschnitt um 0,2 Prozent.
Kurzlink tinyurl.com/yjf5h3nb

Diebstahl im Handel auf Rekordhoch. So lassen sich die 60-seitige EHI-Studie „Inventurdifferenzen 2024" und der am 3. Juli 2024 in Köln durchgeführte EHI-Kongress „Inventur und Sicherheit" zusammenfassen. An der diesjährigen Befragung nahmen 84 Unternehmen teil, die insgesamt 17.426 Verkaufsstellen repräsentieren. Die Inventurdifferenzen stiegen im Jahresvergleich 2023 zu 2022 von 4,6 auf 4,8 Milliarden Euro. Darin enthalten ist ein Anteil der Verluste durch Ladendiebstahl von insgesamt 2,82 Milliarden Euro. Auch die polizeiliche Kriminalstatistik des Jahres 2023 weist einen massiven Anstieg angezeigter Ladendiebstähle um 23,6 Prozent aus. Aus dem durchschnittlichen Schaden aller angezeigten Diebstähle und dem per Inventur festgestellten Schaden ergibt sich, dass jährlich etwa 24 Millionen Ladendiebstähle im Wert von knapp 120 Euro unentdeckt bleiben. Etwa 0,32 Prozent des Branchenumsatzes in Höhe von 485 Mrd. Euro gibt der Handel für Sicherheitsmaßnahmen aus. Dies umfasst Kosten für Kameraüberwachung, Detektivpersonal, Maßnahmen der Artikelsicherung, Schulungen und Testkäufe. Insgesamt gibt der Einzelhandel 1,55 Milliarden Euro zur Reduktion von Inventurdifferenzen aus. ehi.org
Kurzlink tinyurl.com/3syx66rw

Impressum

50. Jahrgang

Herausgeber
Rainer von zur Mühlen
Peter Stürmann

TeMedia Verlags GmbH
Ein Unternehmen der VZM-Gruppe
Alte Heerstraße 1, 53121 Bonn
Telefon: 0228 96293-80
Telefax: 0228 96293-90

Redaktion
redaktion@sicherheits-berater.de
www.sicherheits-berater.de
direkt.sicherheits-berater.de
Bernd Zimmermann
(Chefredaktion, V.i.S.d.P.)
Telefon: 0228 96293-81
chefredaktion@sicherheits-berater.de

Jörg Schulz, Peter Schmidt,
Rochus Zalud

Media-Beratung
Alice M.W. Hoffmann
Telefon: 0228 96293-21
anzeigen@sicherheitsberater.de

Leserservice
info@sicherheits-berater.de
Telefon: 0228 96293-80

Erscheinungsweise
Zweimal monatlich

Preise
Einzelheft: 17,50 € plus Versand
Jahresabo: 294,00 € inkl. Porto
Semesterabo: 25,00 € inkl. Porto
Auslandsabo: 280,00 € zzgl. MWSt. gem. UStG und Versand
Luftpostgebühren auf Anfrage

Abonnementskündigungen sind mit einer Frist von vier Wochen zum Ende des berechneten Bezugszeitraumes möglich.

Druck: Unitedprint.com Vertriebsgesellschaft mbH, 01445 Radebeul

Bildquellen:
S. 293 (Titel) + S. 295 ©wijas,
S. 297 ©Pixel-Shot,
S. 300 ©Cagkan, S. 301 ©jordi2r,
S. 303 ©Jeannette Dietl,
S. 305 ©Björn Wylezich,
S. 308 ©Michael Jung
– alle stock.adobe.com

ISSN 0344-8746

Aktuelle Entwicklungen der EU-Resilienzrechtslage. Die EU arbeitet intensiv an der Homogenisierung ihrer Resilienzrechtslage, insbesondere durch die Richtlinien DORA (Digital Operational Resilience Act) und NIS2 (Network and Information Security Directive). Während diese Initiativen voranschreiten, bleibt die Umsetzung des KRITIS-Dachgesetzes in Deutschland unklar. Eine offizielle Stellungnahme zur Einhaltung der Umsetzungsfrist und Veröffentlichung des Gesetzes steht noch aus, was zu Unsicherheit führt. Beobachter warten gespannt, ob der aktuelle Referentenentwurf umgesetzt oder ein neuer Entwurf vorgelegt wird. VZM-Berater Christian Horres ist der Meinung, dass es noch zu Änderungen kommen wird, die aber nach aktueller Einschätzung nicht sehr umfangreich sein werden. Wir berichten für Sie weiter.

Großrazzien bei Sicherheitsdiensten und Verdacht auf Steuerbetrug in Millionenhöhe kommentiert der ASW Norddeutschland (Allianz für Sicherheit der Wirtschaft e.V.) wie folgt: „Die Verdächtigen stammen ausgerechnet aus dem Sicherheitsgewerbe – und agierten international. Der Steuerschaden liegt bei über 8 Millionen Euro. Betrug in der Branche ist einfach – jeder kann ein Sicherheitsunternehmen ohne Nachweis von gewerblichen Qualifikationen gründen. Wir warten seit mittlerweile sechs Jahren auf ein Sicherheitsgewerbegesetz, dass diese Machenschaften unterbinden sollte." ASWNord.de
Kurzlink: tinyurl.com/ue84t35t

ZVEI-Umfrage: Acht von zehn Befragten ist Sicherheit in den eigenen vier Wänden ein wichtiges Anliegen. Das ergab eine Umfrage der GfK im Auftrag des Verbands der Elektro- und Digitalindustrie ZVEI. 66 Prozent der Befragten planen, in Sicherheitstechnik zu investieren. Rauchwarnmelder stehen hier an erster Stelle (43 %), gefolgt von mechanischem bzw. elektronischem Einbruchschutz (30 %) und Videosicherheitstechnik (26 %). Besonders die Gruppe der unter 30-Jährigen fasst Investitionen in Sicherheitstechnik ins Auge (90 %), bei den 30- bis 39-Jährigen gilt dies für acht von zehn Befragten (79 %). Die Befragung wurde im Mai 2024 durchgeführt. ZVEI.org
Kurzlink: tinyurl.com/5n78yyka

ZU GUTER LETZT

Der OMA-Aufzug

Kürzlich konnte ich in einer Übersichtszeichnung die einzelnen Bezeichnungen und Nummerierungen der Aufzüge in einem Gebäudekomplex herauslesen. Neben dem Feuerwehraufzug, einigen Transport- und den in den Kernbereichen angeordneten Personenaufzügen fand ich den „OMA-Aufzug". Was ist dies für ein Aufzug? Vielleicht im Zeichen der Gleichberechtigung ein Aufzug, den die Ruheständlerinnen des Unternehmens bei einem spontanen Besuch nutzen können, weil dieser barrierefrei und besonders großzügig ausgestattet ist? Oder ist dieser mit einer sehr geringen Fahrgeschwindigkeit und besonders langen Haltezeiten steuerungstechnisch ausgeprägt? Leider habe ich mir aber viel zu viele Gedanken gemacht. Es handelt sich simpel um eine codierte Bezeichnung. Der Hintergrund dafür: In betriebsfreien Zeiten fährt dieser Aufzug auch einen besonderen Sicherheitsbereich in einer Etage an, deren Vorraum zusätzlich einbruchmeldetechnisch überwacht wird, da der tagsüber dort befindliche Empfang bzw. Info-Point nicht besetzt ist. Eine Zwangsläufigkeit gemäß Vorgaben der Norm an Einbruchmeldeanlagen ist wegen der besonderen Bauweise der Aufzugstüren nicht möglich. Durch Dienstanweisung ist geregelt, dass die Mitarbeiter in diesen Zeiten den Aufzug nicht nutzen dürfen. Eben ein **O**hne**M**it**A**rbeiter sich bewegender Aufzug. Tipp von mir: Aufzugsnutzung zeitlich einschränken und vertikale Fahrten in betriebsfreien Zeiten nicht zulassen. Wäre dann ein **NN**-Aufzug (**N**icht **N**utzbarer Aufzug)! Ihnen eine gute Fahrt in den Urlaub, unabhängig davon, in welche Richtung es geht! ::: Rochus Zalud :::