RADAR
CYBER SECURITY

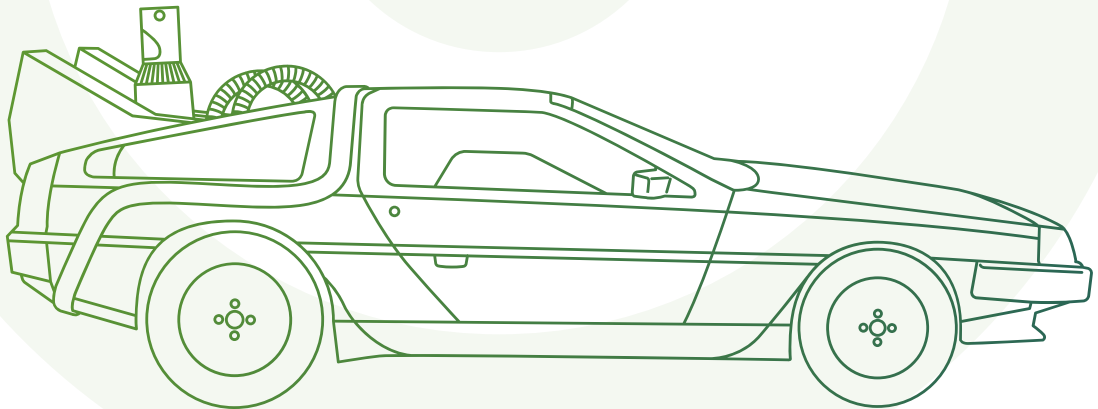
CYBERSECURITY TREND REPORT

2020 im Blick

Ein Blick zurück, um nach vorne zu schauen.

Technologie spielt in alle Aspekte des täglichen Lebens hinein: von A wie Abfallwirtschaft bis Z wie Zugfahren. Damit beeinflusst sie zentrale Bereiche wie Energie- und Wasserversorgung sowie den Gesundheits- und Lebensmittelbereich.

Kaum ein Aspekt unseres Lebens ist nicht von Technologie beeinflusst oder digital verbunden. Wir setzen immer mehr Technologien in Berufs- und Privatleben ein – gleichzeitig werden diese immer komplexer und damit anfälliger für Angriffe und Manipulation. Je größer und komplexer die Infrastruktur, desto angreifbarer sind Unternehmen.



EWIGER DAUERBRENNER

Cyberangriffe und Datendiebstahl bzw. -betrug finden sich seit Jahren unter den Top 10 Risiken des Weltwirtschaftsforums, sowohl in Bezug auf die Wahrscheinlichkeit als auch in Bezug auf die weitreichenden, desaströsen Auswirkungen. Die gefährlichen Auswirkungen, die Cyberangriffe haben können, werden auch weiterhin dafür sorgen, dass sie ein Fixpunkt auf dieser Liste bleiben. Laut der Befragung des deutschen Digitalverbands Bitkom wurden 3 von 4 Unternehmen Opfer von Sabotage, Datendiebstahl oder Spionage. Dadurch entstand der deutschen Wirtschaft ein jährlicher Gesamtschaden von 102,9 Mrd. Euro.

DAS 26-MILLIARDEN-DOLLAR-PROBLEM

Das FBI hat unlängst Zahlen zur Kompromittierung von geschäftlichen und privaten E-Mails veröffentlicht. Seit Juli 2016 beläuft sich der Schaden auf mehr als 26 Milliarden Dollar weltweit, mehr als doppelt so viel wie noch 2018 vermeldet wurde. Die Kompromittierung von E-Mails ist im Vergleich zum Hacken der Infrastruktur eines Unternehmens ein vergleichsweise einfacher und effektiver Weg für Cyberangreifer. Die Nutzung dieses Kommunikationskanals durch personalisierte Nachrichten ermöglicht es, sich leicht als vertrauenswürdiger Mitarbeiter, Kunde oder Partner auszugeben und dann Zugriffsrechte auf ganze Unternehmensinfrastrukturen zu erhalten oder Mitarbeiter zu widerrechtlichen Überweisungen oder Änderung der Kontodaten aufzufordern.

Neue Herausforderungen

DIE GEFAHR LAUERT IMMER UND ÜBERALL

Mitarbeiter arbeiten im Homeoffice, im Zug, am Flughafen, im Hotel oder direkt bei Kunden, sind mobil, greifen von überall auf der Welt auf Firmennetzwerke zu und stellen damit eine immer größere Angriffsfläche und ein steigendes Sicherheitsrisiko für das gesamte Unternehmen dar. Klare Programm- und Richtlinienerstellung, Kommunikation, Risikobewertung, Technologieumsetzung sowie kontinuierliche Überwachung und Bewertung müssen auf die besonderen Herausforderungen im Zusammenhang mit mobilen Geräten zugeschnitten sein.

EIN ANSCHLUSS UNTER DIESER NETZWERKNUMMER

Unternehmen mit vielen Standorten müssen überall für Sicherheit sorgen und Risiken minimieren – in Produktionshallen, Büros oder Filialen. Ansonsten können Schwachstellen bei kleinen Niederlassungen für große Überraschungen sorgen. Gleichzeitig muss der Zugang zum Internet, zu Unternehmens- und Produktionsnetzwerken durchgehend gewährleistet sein. Laut Gartner kostet ein Ausfall Unternehmen durchschnittlich 4.900 Euro pro Minute. Zeit ist Geld, umso mehr, wenn Dienstleistungen und Produkte ausfallen und Einnahmen in Millionenhöhe verloren gehen.

AB IN DIE WOLKE

Mehr Datenverkehr benötigt auch mehr Power. So wandern immer mehr Anwendungen aus dem firmeneigenen Rechenzentrum in die Cloud. Die Absicherung der Cloudumgebung mit den transferierten Daten sowie der Übertragung an sich muss ebenfalls aktiv betrieben werden. Ebenso müssen der Einsatz von Public Clouds und die Risiken möglicher Ausfälle, wie es bei der Google Cloud im März letzten Jahres der Fall war, berücksichtigt werden.

VON ALI G ZU 5G

Die Möglichkeiten von 5G, angefangen von der Datenrate bis zur Zuverlässigkeit, sind verlockend und werden eine Flut an neuen, verbundenen Geräten und dementsprechend noch mehr personenbezogene Daten mit sich bringen. Von E-Health-Apps über Smart Cars bis zur Smart City kennt die Informationssammelwut keine Grenzen. Diese privaten, personenbezogenen Daten müssen vor Missbrauch und Diebstahl entsprechend geschützt werden.

Im Fokus

Cybersecurity ist ein integraler Bestandteil der Unternehmensführung. Denn statt reiner Unterstützungsaufgabe und Sicherstellung, dass alle Systeme reibungslos laufen, hat Sicherheit vielmehr eine geschäftsfördernde Funktion. Cybersecurity hat direkte Auswirkungen auf Ansehen, Aktienkurs, Umsatz, Markenwert, Geschäftsbeziehungen zu Kunden und Partnern sowie Produkteinführungen.

Das technische Herzstück einer Firma ist heutzutage schwer auszumachen. Ist es das IT Security Team, das Rechenzentrum, der E-Mail-Server? Sind es die Source Codes, Patente, Kundendaten oder die Anwendungen in der Cloud? Mit jeder neuen Technologie wird das Thema Sicherheit für Unternehmen noch komplexer. Aus diesem Grund werden neue Zugänge zu Cybersecurity benötigt, um konkurrenzfähig zu bleiben und das Potenzial der Wertschöpfung durch die Digitalisierung effizient zu nutzen.

Radar Cyber Security Ausblick 2020

WAS CYBERSECURITY-PROFIS WISSEN MÜSSEN:

1 GESUNDHEITS-CHECK

Als Teil des digitalen Gesundheitsreports im Unternehmen gehören Update- bzw. Patchzyklen sowie regelmäßige Datensicherungen etabliert. Auch die Installation und sachgerechte Konfiguration von Anwendungen, IoT-Geräten und Protokollen ist dafür erforderlich.

Patchzyklen müssen zuverlässig und zügig umgesetzt werden – von der Verteilung bis zum Einsatz. Denn nur so ist sichergestellt, dass etwaige Schwachstellen schnell beseitigt werden können. Die Sicherheit muss während der gesamten Lebensdauer eines Netzwerks oder Geräts gewährleistet und Cybersecuritymaßnahmen müssen laufend aktualisiert werden.

2 AUF DIE PLÄTZE, FERTIG, LOS!

Datenschutzmechanismen müssen intakt sein, je schneller diese greifen, desto besser. Aber viele Hacks, die dieses Jahr bekannt wurden, wurden im Schnitt erst nach sechs Monaten erkannt – in Extremfällen gar erst Jahre später. Laut EU-DSGVO müssen Datenschutzverstöße innerhalb von 72 Stunden gemeldet werden, ansonsten drohen Strafen. Abgesehen von gesetzlichen Auflagen müssen Schwachstellen in Unternehmens- und Produktionssystemen umgehend erkannt werden, um vor schadhaften Aktivitäten, Manipulationen und Diebstahl geschützt zu sein – nicht erst nach Tagen oder Wochen. Diese Reaktionszeit und der notwendige Aufwand zur Beseitigung von Incidents können durch den Einsatz von Sicherheitsmodulen erheblich reduziert werden.

3

WIE HEISST DAS ZAUBERWORT? DATEN!

Informationen und Daten haben für Unternehmen großen Wert und sind zugleich auch Verbindlichkeiten, die geschützt werden müssen. Mehr als ein Jahr nach dem Inkrafttreten der EU-DSGVO sind laut International Association of Privacy Professionals, kurz IAPP, insgesamt mehr als 89.000 Datensicherheitsverstöße verzeichnet worden. Bislang wurden laut GDPR Enforcement Tracker, www.enforcementtracker.com, im Rahmen der EU-DSGVO europaweit Strafen in Höhe von mehr als 350 Millionen Euro verhängt. In Deutschland beläuft sich die Summe an EU-DSGVO Strafzahlungen auf ca. 24,6 Mio. €, in Österreich auf ca. 18,1 Mio. €. Wie hoch die Dunkelziffer an nicht erkannten und nicht gemeldeten Vorfällen ist, kann nur vermutet werden. Die Bedeutung von Datenschutz wird im Hinblick auf die zunehmende Vernetzung auch in kritischen Bereichen weiter steigen.

4

ALLGEMEINE IT-VERUNSICHERUNG

Wissen ist Macht, auch was Inventar und Kontrolle von Services, Prozessen, Hardware und Software eines Unternehmens anbelangt. IT-Sicherheit kann verbessert werden, indem bisher unbekannte Assets aufgespürt werden. Denn eine Übersicht über die Geräte, die sich im Firmennetzwerk befinden, ist für die Einhaltung von Compliance-Richtlinien unumgänglich. Dies umfasst auch die Meldung von gestohlenen oder defekten Geräten.

5

KEIN ZUTRITT FÜR UNBEFUGTE

Die Überwachung des Zutritts beschränkt sich nicht nur auf die Sicherung von Gebäuden, Räumen und physischen IT-Ressourcen, sondern umfasst auch die Beschränkung von Verbindungen zu Computernetzwerken, Systemdateien und Daten. So wird reguliert, wer was im Firmennetzwerk sehen oder nutzen darf. Denn nicht alle Bereiche, Geräte und Server müssen für alle Mitarbeiter zugänglich sein. Angemessene Autorisierungen, Berechtigungen, Alarmierungen und Audits regeln den Zugriff bzw. Zutritt zu Gebäuden und sensiblen Bereichen.

6

WER BIST DENN DU?

Logins und Datenverkehr müssen nicht nur gecheckt werden, wenn sie von externen Quellen kommen bzw. nach extern übermittelt werden, sondern auch innerhalb des Unternehmens überwacht werden. Grundlage für Sicherheitsfragen ist das regelmäßige Ändern von Passwörtern bzw. ist das Ändern von Standardpasswörtern vor allem bei IoT-Geräten unerlässlich. Diese Sicherheitsrichtlinien müssen lückenlos unternehmensweit durchgesetzt werden. Wenn ein Verstoß gegen diese erkannt wird, müssen korrigierende Maßnahmen umgehend durchgeführt werden. Eine Zwei-Faktoren-Authentifizierung steigert zusätzlich die Sicherheit. Dieser zweite Schritt macht es Angreifern deutlich schwerer, Accounts zu hacken. Zwecks Authentifizierung werden Benachrichtigungen via SMS, Apps, biometrische Daten wie Gesichtserkennung sowie Security Keys eingesetzt.

7 KLARE REGELN

Dank Use Cases kann die automatische Überwachung des Status von Anlagen und Netzwerken auf Basis von relevanten Werten und Indikatoren zur Cybersecurity beitragen. Das steigert den Sicherheitszustand und erleichtert und beschleunigt die Erkennung von Anomalien und damit wirklich bösartigen und kritischen Attacken und Risiken. Use Cases können weiterentwickelt werden, um Angriffsvektoren frühzeitig zu erkennen und festzumachen. Sie sind Teil des Schlüssels für ein erfolgreiches Sicherheitskonzept. Es stellt sicher, dass jedes implementierte Sicherheitsmodul und -tool und jeder entwickelte Use Case nutzbar und wertvoll ist.

8 SICHERHEITS-PARADIGMENWECHSEL

Weg von Verfügbarkeit hin zur umfassenden Sicherheit heißt es für Unternehmen, die Teil der kritischen Infrastruktur sind. Darunter fallen Anbieter und Betreiber aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Mit weiteren Gesetzen werden diese Auflagen auch auf die Rüstungsindustrie, Kultur- und Medienunternehmen sowie Abfallwirtschaft ausgedehnt. So gilt es nicht nur die EU-DSGVO einzuhalten, sondern auch das NIS-Gesetz bzw. in Deutschland das IT-Sicherheitsgesetz 2.0. So sind Unternehmen verpflichtet, umfangreiche Sicherheitsmaßnahmen umzusetzen und ihre Wirksamkeit nachzuweisen. Für deutsche KRITIS-Unternehmen bedeutet das zusätzlich den dezidierten Einsatz von Systemen zur Angriffserkennung auf dem Stand der Technik.

9 MEHR GERÄTE, MEHR PROBLEME

Die Vielzahl an Geräten und Anwendungen, darunter immer mehr IoT-Geräte, birgt unzählige Risiken. Die Absicherung der Verbindungen zu Rechenzentren und Clouds hat oberste Priorität. Bei so vielen Geräten stellt sich auch immer wieder die Frage: Aufbewahren oder in den Müll damit? Nicht mehr benötigte Geräte, die möglicherweise vertrauliche Daten gespeichert haben können, wie z.B. Drucker und Kopierer, gehören fachgemäß und sicher entsorgt.

10 MINI-GERÄTE UND BIG DATA

IoT-Geräte haben Prozesse verändert und Services neu gestaltet. Das IoNT, Internet of Nano Things, wird noch tiefere Einblicke in Produktions- und Unternehmensbereiche liefern, gleichzeitig auch die Datenflut in den kommenden Jahren potenzieren. Die Geräte unterscheiden sich von IoT deutlich in ihrer Größe und sind in Design und Fertigung extrem raffiniert und ausgeklügelt. Sie messen und überwachen Temperatur, Luftfeuchtigkeit, Wasserqualität oder Abgaswerte. Neben hochsensiblen Produktionsstätten finden sich Nanosensoren verstärkt in Smart Homes, Smart Cars, im Gesundheitsbereich oder der Landwirtschaft. Sowohl die Geräte, die auch kritische bzw. personenbezogene Daten sammeln, als auch ihre digitale Anbindung ans Netzwerk müssen von Unternehmen strikt überwacht und geschützt werden.

Cybersecurity-Checkliste

CYBERSECURITY, WAS NUN?

Ein ganzheitlicher Sicherheitsansatz muss her, um Menschen und Unternehmen vor immer größeren und umfassenderen Bedrohungen zu schützen. Jeder Bereich kann zum potenziellen Einfallstor für Cyberangriffe werden. Durch die globale Vernetzung und Industrie 4.0 benötigt es einen umfassenden Ansatz zum Schutz der IT und OT vor Cyberattacken. Denn nur so können Unternehmen eine widerstandsfähige IT- und OT-Infrastruktur schaffen und Risiken für Betriebsausfälle minimieren.

VORSICHT STATT NACHSICHT

Jeder zehnte Betrieb trifft keine Vorkehrungen, um sich gegen IT-Sicherheitsvorfälle zu schützen, so die Statistik Austria. In Deutschland wurde laut TÜV-Umfrage jede achte Firma in den letzten zwölf Monaten Ziel eines systematischen Cyberangriffs.

Die Risiken für Unternehmen bleiben auch weiterhin konstant hoch. Die Bedrohungslandschaft ändert sich ständig und macht den Einsatz von Früherkennungssystemen erforderlich, auch im Bereich der kritischen Infrastruktur. Nach den Datenschutzauflagen der EU-DSGVO sind mit dem NIS-Gesetz bzw. dem neuen IT-Sicherheitsgesetz 2.0 nun kritische Infrastrukturen im Fokus. Sie müssen ihre Systeme umfassend, mit Systemen zur Angriffserkennung, und nach Stand der Technik mit den richtigen Modulen und Tools schützen. Das umfasst Module wie Log Data Analytics, auch SIEM genannt, Network Behavior Analytics, kurz NBA, sowie Vulnerability Management und Compliance, kurz VMC. Die Cybersecuritymaßnahmen müssen laufend aktualisiert und Tools und Methoden ständig weiterentwickelt und verfeinert werden.

Cybersecurity ist ein Marathon, kein Sprint.

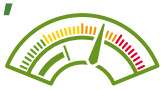
MIT VEREINTEN KRÄFTEN

Cybersecurity geht alle an. Aus diesem Grund müssen alle Bereiche des Unternehmens dafür sensibilisiert werden. Oftmals nutzen Angreifer Unwissenheit und Gutgläubigkeit von Mitarbeitern aus. Es ist daher für jedes Unternehmen wichtig, die eigenen Mitarbeiter für sicherheitsrelevante Themen zu sensibilisieren. Schon aufgrund der Haftung im Rahmen der EU-DSGVO müssen Bedeutung und Verantwortung der Sicherheitsaspekte auch im Management verankert sein. IT-Sicherheitsmodule, Datenschutz und Security-Awareness gehen Hand in Hand.

KEINE FRAGE DER GRÖSSE

In Sachen Cybersecurity gibt es keine kleinen oder uninteressanten Ziele. Viele mittelständische Betriebe geraten als bekannte Innovations-, Technologie- und Wirtschaftstreiber regelmäßig ins Visier von Angreifern. Der Schaden hat auf große Betriebe wie auch auf den Mittelstand verheerende Auswirkungen. Speziell viele mittelständische Unternehmen investieren nicht oder nicht ausreichend in IT-Sicherheit. Ein Ausfall kann so für Unternehmen auch schnell zum Konkursfall werden. Frühzeitig in Cybersecurity und die richtigen Erkennungsmodule zu investieren kann sich daher schon kurzfristig lohnen, um Angriffe zu vermeiden.

EINE ÜBERSICHT, UM ALLES ZU SEHEN



Unternehmen unterliegen oft dem Trugschluss, dass viele unterschiedliche Lösungen auch mehr Sicherheit bedeuten. Eine Umfrage der IT-Forschungs- und Analystenfirma ESG zeigt, dass 55 Prozent der Unternehmen mehr als 25 verschiedene Cybersecurity-Produkte im Einsatz haben. Mehr Sicherheitswerkzeuge steigern nicht automatisch die Sicherheit, meist hat dies den gegenteiligen Effekt. Denn diese Men-

ge an Tools erzeugt neben vielen Daten auch eine hohe Arbeitsbelastung für die meist wenigen Sicherheitsfachkräfte in Unternehmen. Das führt dazu, dass nicht genügend Zeit bleibt, diese Werkzeuge optimal zu nutzen. Denn all diese Ergebnisse und Daten unterschiedlichster Lösungen müssen gesichtet, ausgewertet und Auffälligkeiten erkannt werden. Eine Übersicht wie das Risk & Security Cockpit, das sämtliche Ereignisse mittels Machine Learning korreliert, dann auswertet und bündelt, macht die Arbeit nicht nur effizienter, sondern reduziert Bedrohungen und Risiken für Unternehmen. Erleichterung schaffen zudem Use Cases, um Risiken schon frühzeitig zu erkennen. Zusätzlich reichern die Experten aus dem Cyber Defense Center von Radar Cyber Security die Daten mit wichtigen Informationen und Anleitungen an.

KRISENPLAN

Die richtigen Cybersecurity-Tools machen den Unterschied, um langfristig für Sicherheit zu sorgen. Neben dem langfristigen Sicherheitszugang und Sicherheitskonzept braucht es eine Strategie für die Reaktion auf kritische Sicherheitsfälle.

Im Notfallplan finden sich die durchzuführenden Maßnahmen und Handlungsanweisungen, um Schäden zu begrenzen oder abzuwenden. Vorfälle, bei denen Notfallpläne zum Einsatz kommen, sind z.B. Stromausfälle, technische Störungen, Feuer, Einbruch, Vandalismus, Hackerangriffe, kriminelle Handlungen, Personalausfall oder Bedienungsfehler. Darin sind technische Anweisungen, Verantwortlichkeiten, Alarmierungsketten, Maßnahmenlisten, Kommunikationsregelungen, Kontaktinformationen oder Maßnahmen für die schnelle Beschaffung von Ersatzteilen angeführt. Der Notfallplan umfasst immer sowohl technische als auch organisatorische Informationen. Dank eines Plans können Unternehmen auf solche außergewöhnlichen, kritischen Ereignisse angemessen und schnell reagieren. Mittels Firefighting und Forensik unterstützt Radar Cyber Security Kunden mit Empfehlungen zur Behebung.

CYBER THREAT HUNTING UND ORCHESTRATION

Von der Reaktion über die Früherkennung zu den nächsten Schritten

Im Bereich Cybersecurity reicht es schon lange nicht mehr aus, nur auf Angriffe zu reagieren. Neben der Früherkennung setzt Radar Cyber Security auch verstärkt auf das proaktive Cyber Threat Hunting, dem Suchen nach Bedrohungen und böswilligen Aktivitäten, mittels Machine Learning. Ziel ist es, anstatt nur auf Warnungen und Verstöße zu reagieren, schon frühzeitig Gefahren einzudämmen und Risiken zu minimieren. Cyber Threat Hunting ersetzt allerdings keine IT- oder OT-Security-Monitoring-Module, vielmehr ergänzt es diese bei der Früherkennung.

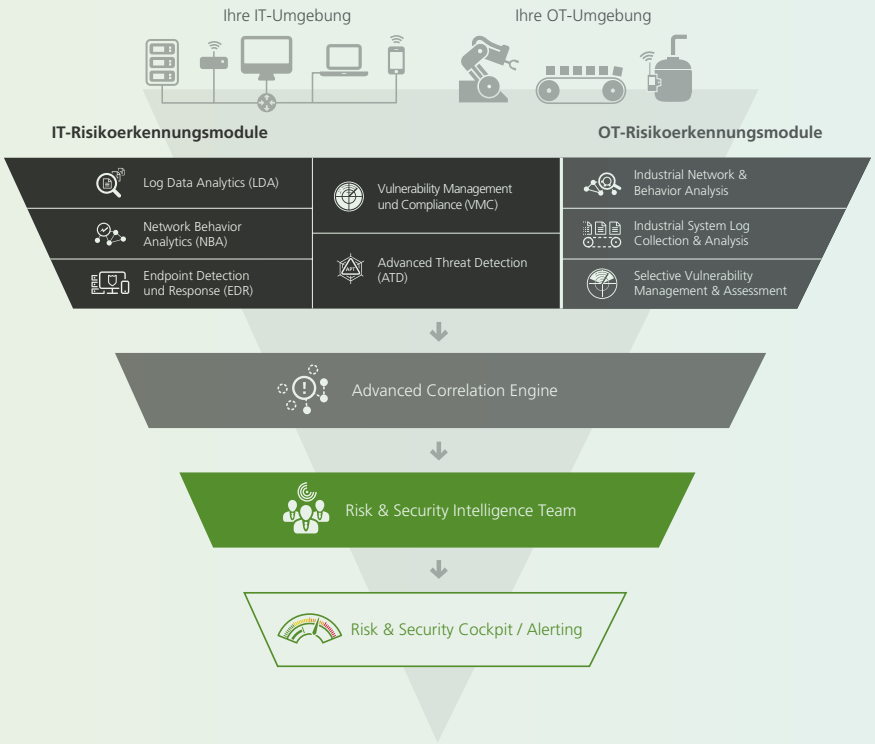
RAIN

Radar Analytics Interface

Mit RAIN, dem Radar Analytics Interface, gewinnen Sicherheitsteams in Unternehmen und CDC-Experten einen noch tieferen Einblick in sämtliche Daten der Systeme und können diese anschaulich visualisieren, um diese optimal zu nutzen. Umfassende Drill-Down- und Korrelierungsfunktionalitäten ermöglichen es, sehr komplexe Abfragen auszuführen – unterstützt durch eine grafische Darstellung der Beziehungen zwischen den Elementen. Sobald bestimmte Verhaltensmuster von Malware erkannt werden, können Experten neue Regeln erstellen.

Das macht RAIN noch intelligenter und effektiver im Erkennen von Bedrohungen und ermöglicht es, Sicherheitsbestrebungen und Risikobehebung optimal zu orchestrieren.

Cybersecurity: Build or buy? Radar Managed Services vs. Radar Platform



IT- UND OT-SICHERHEIT ALS MANAGED SERVICES

Als Cybersecurity-Dienstleister bietet Radar Cyber Security ein ganzheitliches IT und OT Security Monitoring als Standardservice. Somit sind Kunden dank dem Radar Risk & Security Cockpit immer up to date was ihre IT- und OT-Risiken inklusive Echtzeit-Alarmierung betrifft. Bei Kunden ist eine Hardware samt modernster Technologien im Einsatz. Top geschulte Experten sind 24/7 verfügbar. Durch Managed Services werden außerdem Prozesse und IT-Infrastruktur verbessert.

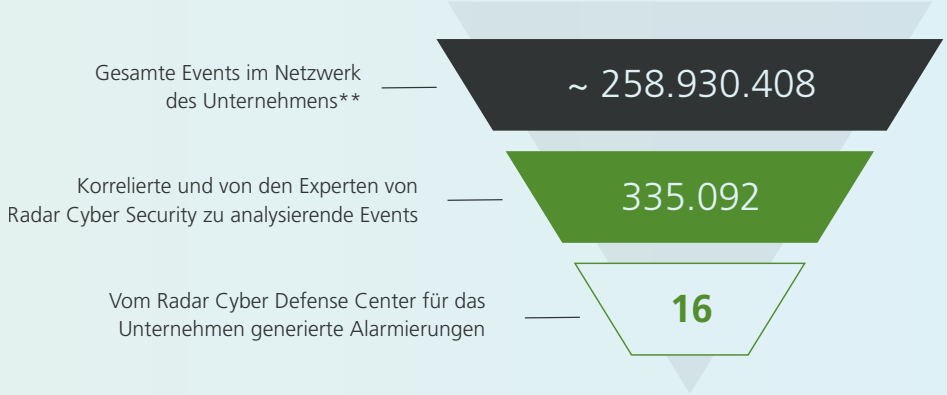
- → Kostenreduktion: Operating und Maintenance
- → Integrierte Gesamtlösung
- → Eingespielte Analyseprozesse
- → Laufend aktualisierte Threat Intelligence
- → Radar Risk & Security Cockpit mit Übersicht der IT-Risiken inkl. Echtzeit-Alarmierung
- → Keine weiteren personellen Ressourcen: Fachkräfte für ein eigenes CDC
- → Flexibilität und Skalierbarkeit
- → Erfahrung durch einen professionellen Anbieter

AUFBAU EINES EIGENEN CDCS MIT DER RADAR PLATFORM

Die Radar Platform gibt Ihnen Cyber Security Detection Technology der nächsten Generation für Ihr eigenes Cyber Defense Center (CDC) an die Hand. Es ist ein einzigartiges Komplettpaket für ein effizientes und effektives Cyber Defense Center bzw. Security Operations Center (SOC).

- → Gesamtpaket aus Hardware und Software – optional samt Equipment
- → Unterstützung in allen Phasen: Planung und Implementierung bis hin zur Integration und laufenden Verbesserung wie Security System und Workflows
- → Anpassung an Kundenbedürfnisse: neueste Updates, integrierte Threat Intelligence und laufende Verbesserungen
- → Empowerment: Service und/oder Sales

Managed Security Services mit NBA & LDA*



*verfügbar als On Premise, Cloud, Virtual
**Werte beziehen sich auf den Monatsdurchschnitt eines Kunden (> 10.000 Mitarbeiter) in 2019

RADAR CYBER SECURITY | Safeguard your digital journey.

Radar Cyber Security ist Europas führendes Technologieunternehmen im Bereich Detection & Response. Im Mittelpunkt steht die zeitnahe Erkennung von Risiken für die Sicherheit der IT und OT von Unternehmen und Behörden als Solution oder als Managed Service. Basis dafür ist eine hochmoderne, eigenentwickelte Technologieplattform mit der Kunden ihr Cyber Defense Center (CDC) aufbauen können oder die in Kombination mit Security-Analyseexperten, bewährten Prozessen und Best Practices als CDC as a Service zur Verfügung steht. Das Ergebnis: Eine besonders effektive und effiziente Verbesserung von IT-Sicherheit und -Risikomanagement, kontinuierliches IT und OT Security Monitoring und ein auf Knopfdruck verfügbarer Überblick über die sicherheitsrelevanten Informationen in der gesamten IT- und OT-Landschaft einer Organisation.

Radar Cyber Security HQ
Zieglergasse 6
1070 Wien
Österreich

T: +43 (1) 929 12 71-0
F: +43 (1) 929 12 71-710
E: sales@radarcs.com
www.radarcs.com

Radar Cyber Security Deutschland
Taunustor 1
60310 Frankfurt am Main
Deutschland

T: +49 (69) 2443424 655
F: +49 (69) 2443424 150
E: sales_germany@radarcs.com
www.radarcs.com/de

Radar Cyber Security Schweiz/Liechtenstein
Schaanerstrasse 1
9490 Vaduz
Liechtenstein

T: +423 237 90 90
F: +423 237 74 99
E: sales_switzerland@radarcs.com
www.radarcs.com/ch

PUBLIC

R_CYBER_2019_DE_1