DIE CYBERSICHERHEITSSERVICES VON MOTOROLA SOLUTIONS

MOTOROLA SOLUTIONS

AKTUELLER TREND VS. **GÄNGIGE PRAXIS**

87%
UNSERER KUNDEN HABEN EIN MITTLERES ODER SEHR GROSSES VERTRAUEN IN DIE CYBERSICHERHEIT IHRER FUNKANLAGEN ZU RECHT? DENN NUR...

53%
FÜHREN EIN AKTIVES SICHERHEITS-MONITORING DURCH

48%
DOKUMENTIEREN IHRE SICHERHEITS-REGELN UND -VERFAHREN

42%
PATCHEN IHRE FUNKANLAGEN

30%
NEHMEN REGEL-MÄSSIG RISIKOBE-WERTUNGEN VOR

22%
FÜHREN KEINE DER VORSTEHENDEN MASSNAHMEN DURCH

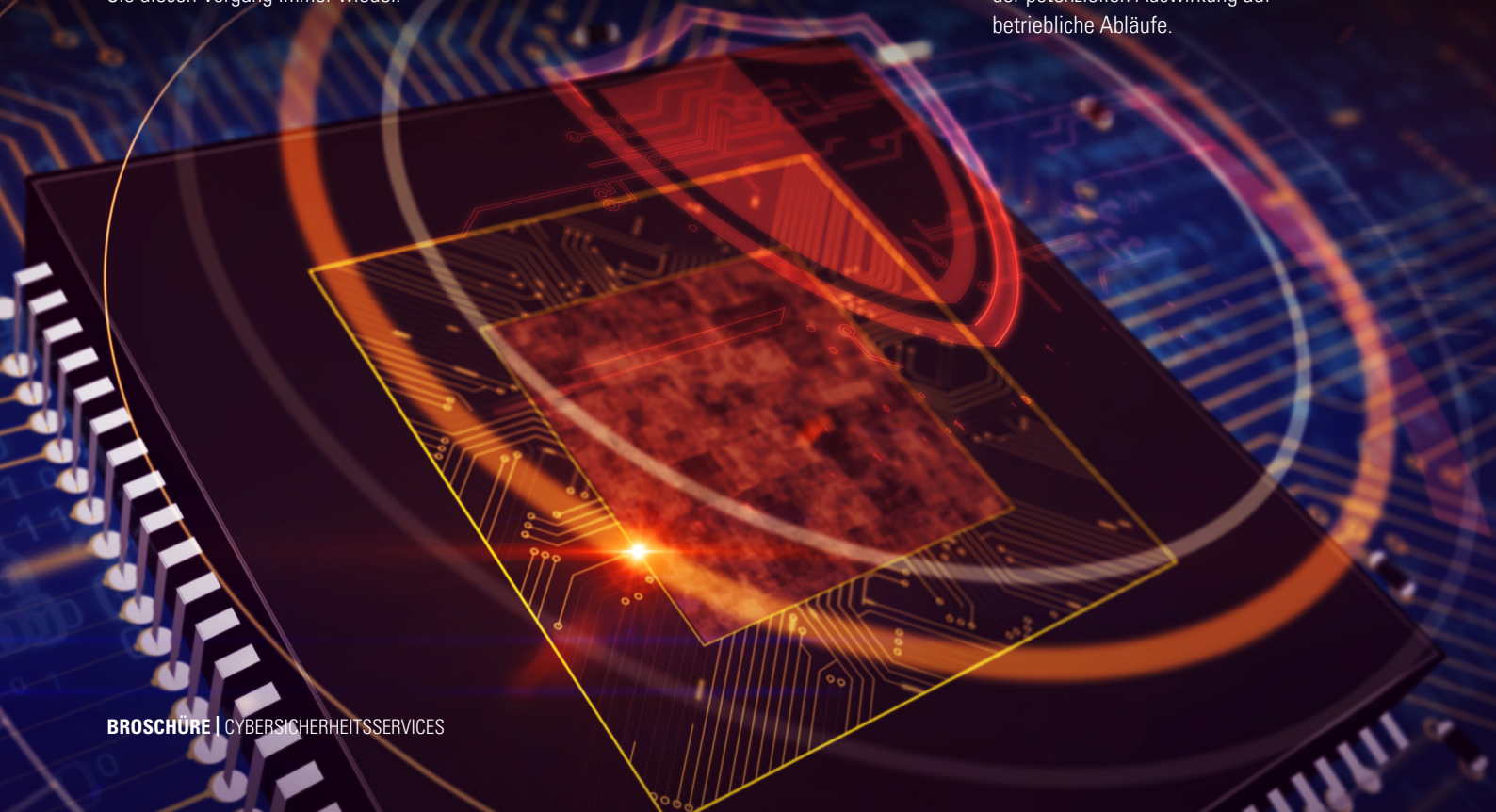
Sämtliche Angaben stammen aus der Studie "LMR System Management Benchmark" von Motorola Solutions (2018)

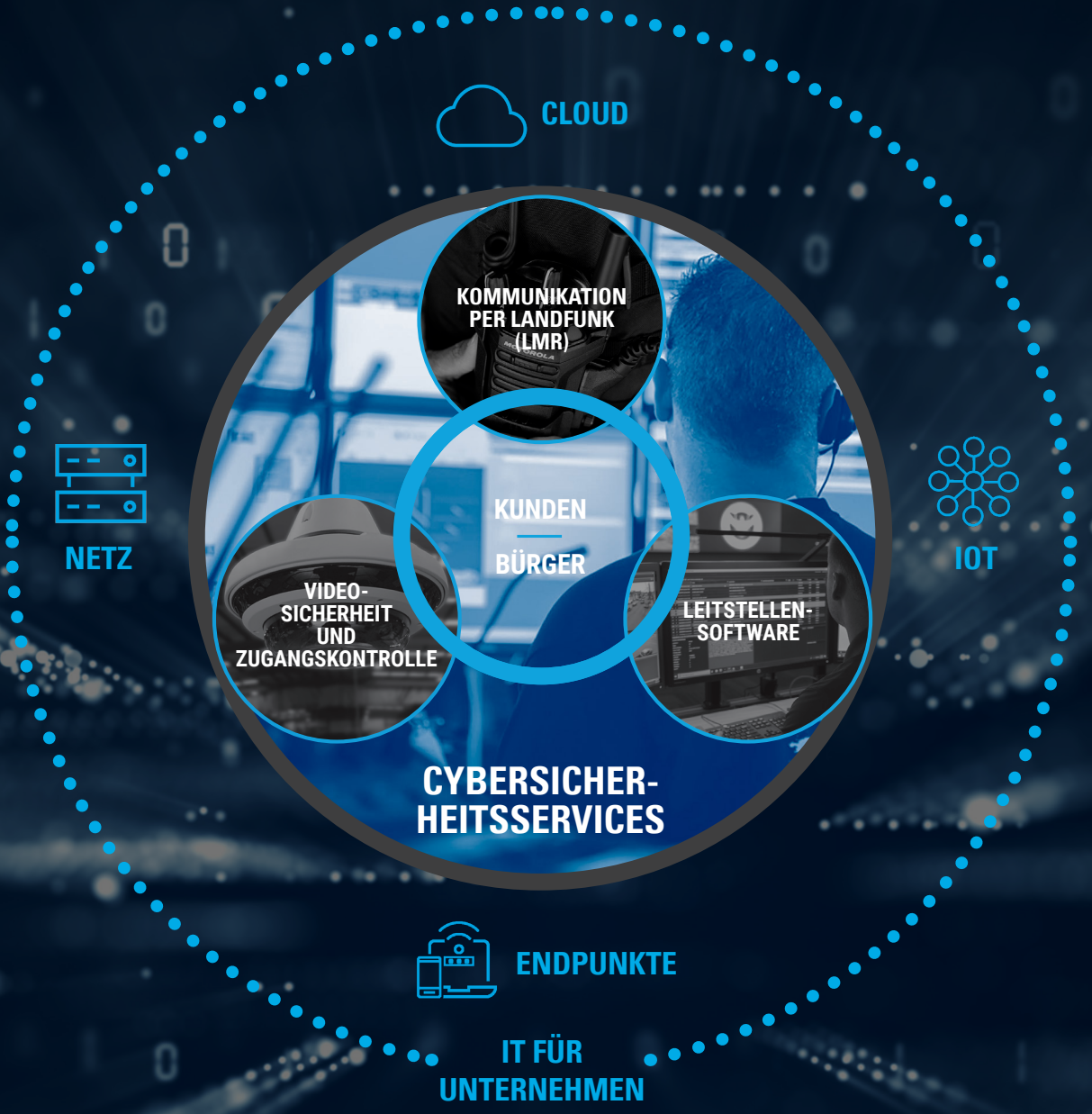
DIE CYBER-BEDROHUNGEN FÜR DIE ÖKOSYSTEME DER ÖFFENTLICHEN SICHERHEIT NEHMEN IMMER WEITER ZU. DOCH NICHT ALLE ORGANISATIONEN HALTEN MIT DEN ERFORDERLICHEN SCHUTZMASSNAHMEN SCHRITT. UM DEN CYBERKRIMINELLEN DAS HANDWERK ZU LEGEN, IST ENTSCHLOSSENES HANDELN GEFRAGT. DIE „CYBERHYGIENE" MUSS ÜBERALL AUF DEN PRÜFSTAND GESTELLT WERDEN.

Keine Organisation ist gegen die zunehmende globale Bedrohung durch Internetkriminalität gefeit. So gut wie alle Nachrichtendienste der Welt haben Verhaltensrichtlinien für virtuelle Bedrohungssituationen veröffentlicht. Bei näherer Betrachtung drehen sich diese Hinweise fast immer um dieselben Punkte: Kümmern Sie sich um das Grundlegende, testen Sie es und wiederholen Sie diesen Vorgang immer wieder.

Wir bei Motorola Solutions wissen, dass die IT-Umgebung Ihrer Organisation und Ihr einsatzkritisches Kommunikationsnetzwerk direkt voneinander abhängig sind. Mit unseren Cybersecurity-Lösungen stellen wir über die geeigneten Werkzeuge und Supportleistungen sicher, dass beide Systeme stabil und geschützt bleiben.

Unser Team erstellt einen auf Ihre Ziele abgestimmten Cybersecurity-Fahrplan, mit dem Sie die Übereinstimmung Ihrer Abläufe mit internationalen Informationssicherheitsvorschriften und Branchenrichtlinien dokumentieren. Der Fahrplan unterstützt Sie auch bei der Verbesserung Ihrer Sicherheitskontrollen und priorisiert diese nach dem Schweregrad der potenziellen Auswirkung auf betriebliche Abläufe.





MOTOROLA SOLUTIONS IST IHR GLOBALER PARTNER FÜR CYBERSICHERHEITS-DIENSTLEISTUNGEN. UNSER INTEGRIERTES PORTFOLIO IST AUF LOKALE UND NATIONALE RAHMENBEDINGUNGEN ABGESTIMMT, IDENTIFIZIERT LÜCKEN IN SICHERHEITSPROGRAMMEN UND ERKENNT BEDROHUNGEN IN NETZWERKEN. SO SIND UNSERE KUNDEN JEDERZEIT AUF JEDE LAGE VORBEREITET.

BERATUNG

Wir unterstützen Sie auf dem Weg zu lückenlosem Schutz und einer sicheren Strategie gegen Bedrohungen aus dem Internet.

MANAGED DETECTION & RESPONSE (MDR)

MDR erkennt Bedrohungen für Ihre Netze und Ihre Infrastruktur – etwa durch Ransomware – noch bevor sie zum Problem werden. Diese werden blockiert und unterbunden.

SICHERHEITSUPDATES

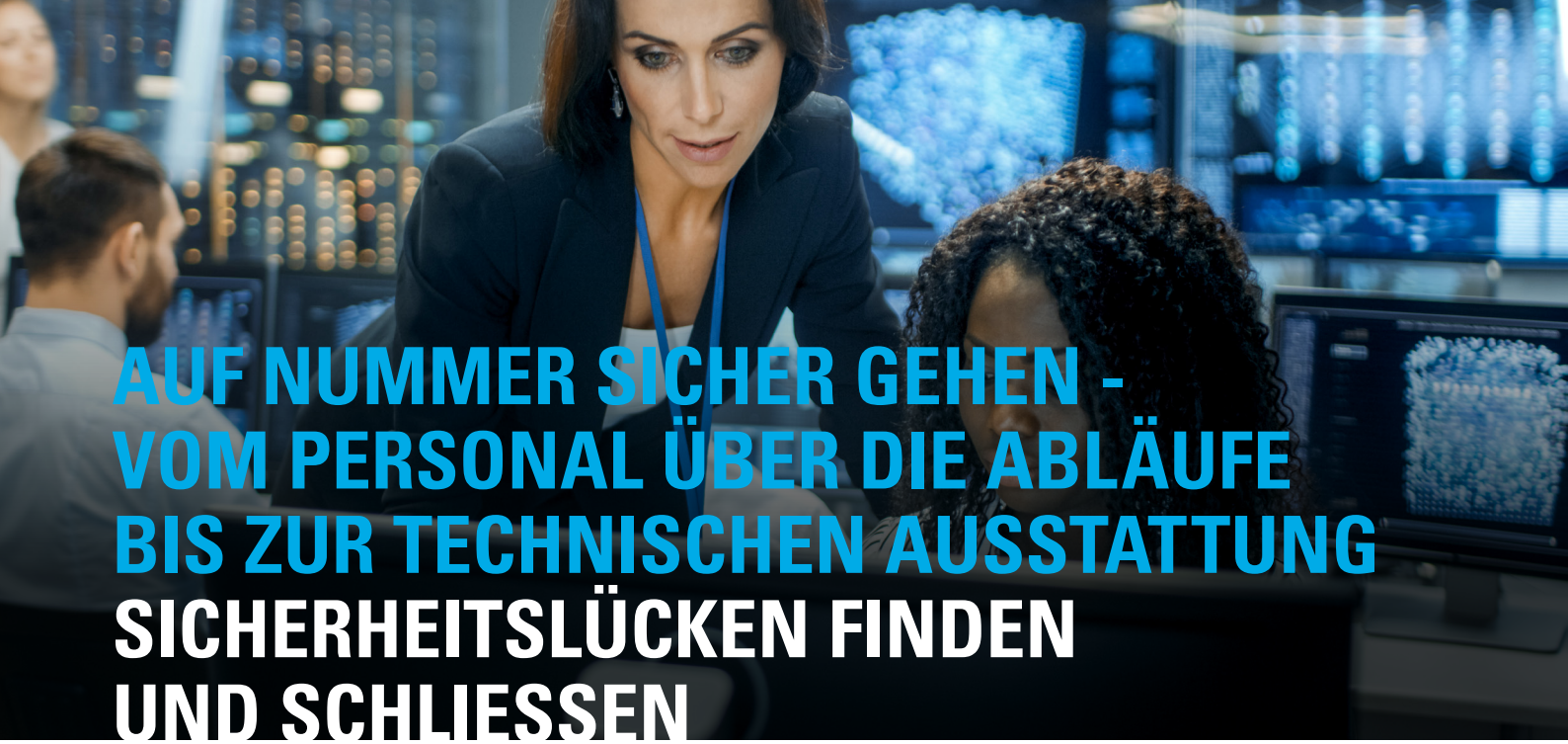
Das sogenannte Patching gehört zu den effektivsten Methoden, um Gefahren aus dem Internet abzuwehren.

VERSCHLÜSSELUNG UND AUTHENTIFZIERUNG

Gewähren Sie nur den von Ihnen ausgewählten Geräten Zugang zu Ihrem Kommunikationsnetz. So bleibt Ihre Kommunikation sicher!

SCHULUNG UND FORTBILDUNG

Mit unseren Schulungen bleiben Sie immer in der Lage, Cyberkriminalität zu verstehen, abzuwehren und ihr vorzubeugen.



AUF NUMMER SICHER GEHEN - VOM PERSONAL ÜBER DIE ABLÄUFE BIS ZUR TECHNISCHEN AUSSTATTUNG SICHERHEITSLÜCKEN FINDEN UND SCHLIESSEN

Motorola Solutions bietet vielfältige Optionen zum Schutz Ihrer Geräte und Ihrer IT-Systeme an und bindet hierbei nicht nur aktuelle Forschungsergebnisse, sondern auch die technische Tiefenanalyse mit ein. Wir prüfen alle verfügbaren Informationen, Kontrollmängel, Systemfehlkonfigurationen und -schwachstellen und simulieren dabei auch böswillige Hackerangriffe, etwa durch Penetrationstests, Schwachstellenprüfungen, szenariobasierte Tests, Reifegradprüfungen und Tabletop-Übungen.

30%
FÜHREN REGELMÄSSIGE RISIKOANALYSEN DURCH

ERKENNEN
SCHWACHSTELLEN IDENTIFIZIEREN

Verschaffen Sie sich einen umfassenden Überblick darüber, wie gut Ihre Sicherheitskontrollen, -richtlinien und -verfahren Ihr Unternehmensnetzwerk, Ihre Cloud-Umgebungen, Ihre Endgeräte und Ihre öffentlichen Sicherheitsnetzwerke schützen.

ANALYSIEREN
REPLIZIEREN VON BEDROHUNGEN

Wir stellen interne und externe Bedrohungen für Ihre Netzwerke, Anwendungen und physischen Standorte nach und zeigen Ihnen dadurch potenzielle Angriffspunkte auf, die Hacker oder böswillige Insider ausnutzen könnten.

UNTERSUCHEN
EXPERTENWISSEN IM BEREICH SICHERHEIT

Wir verwenden eine vielschichtige Strategie, die das Fachwissen unserer spezialisierten Teams mit einer Vielzahl ausgefeilter technischer Tools und Fähigkeiten kombiniert.

VOLLSTÄNDIG KOMPATIBEL MIT DEM CYBERSECURITY-FRAMEWORK NIST

WIEDERHOLBARER PROZESS, KONTINUIERLICHE LAGEERKENNUNG UND BEWERTUNG

VORAB-ANALYSE	VOR-ORT-PRÜFUNG	ABSCHLIESSENDE AUSWERTUNG
BETRIEBLICHE ANFORDERUNGEN VERSTEHEN, ZIELE DEFINIEREN	DURCHFÜHRUNG DER NIST-ANPASSUNG, TECHNISCHE SCHWACHSTELLEN UND BEDROHUNGEN BEWERTUNG RELEVANTER INFORMATIONEN	ROADMAP UND EMPFEHLUNGEN ERSTELLEN
Aktuelle Sicht der Betriebsabläufe und Cybersecurity-Praktiken	Datenerhebung	Lückenanalyse und Berichterstattung
Geplant, Bestätigung der Ziele, Ergebnisse und Erwartungen	Abläufe, Tools, Fähigkeiten und Prozessanpassung	Fehlerbehebung

LAUFENDE STRATEGIE ZUM SCHUTZ VOR CYBERANGRIFFEN

GANZHEITLICHE PRÜFUNG IHRER TECHNOLOGIEUMGEBUNG FÜR DIE ÖFFENTLICHE SICHERHEIT

MANAGED SECURITY-PLATTFORM ActiveEye: MEHR SICHTBARKEIT FÜR IHRE FUNKSYSTEME, PHYSISCHEN IT-NETZ-WERKE UND CLOUDBASIERTEN NETZE

Unsere erweiterte Sicherheitsplattform ActiveEye bietet einen umfassenden Überblick über Ihre Systeme und Netzwerke sowie viele zusätzliche Features. Nach dem Login erhalten Sie schnell und direkt einen Überblick über alle Ereignisse, die sich in Ihrer IT-Umgebung abspielen. So behalten Sie jederzeit den Überblick über alle Maßnahmen, die zum Schutz wichtiger Systemressourcen vorgenommen wurden. ActiveEye archiviert Bedrohungen in einer eigenen Datenbank und erkennt aktiv jeden ungewöhnlichen Vorgang, von dem eine Gefahr ausgehen könnte. Ob Office 365, Google Workspace, AWS oder Azure - ActiveEye schützt Ihre Ressourcen auch beim Umstieg in die Cloud!

53%
FÜHREN EIN AKTIVES SICHERHEITS-MONITORING DURCH

ENTDECKEN & ZUSAMMENFÜHREN

Netzwerk, Endpunkt & Cloud

Schwachstellen erkennen

Integrierte Lösungen von Motorola Solutions

ANALYSIEREN & UNTERSUCHEN

Gefahren erkennen

ActiveEye

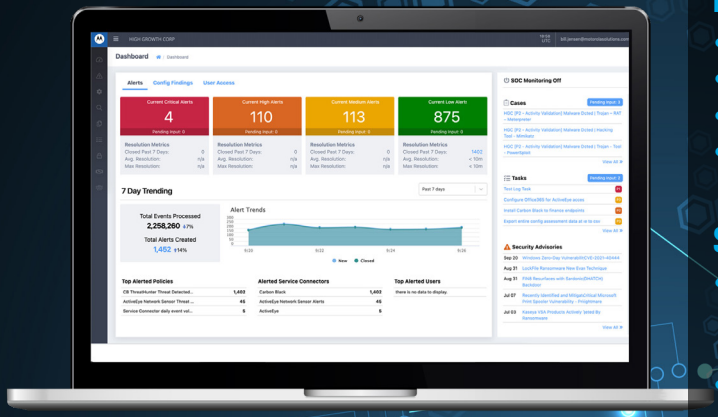
24/7 Untersuchung

HELFEN & REAGIEREN

Bedrohungen abwehren

Gemeinsam verwaltetes Portal

Kundenspezifische Benachrichtigungen



MANAGED NETWORK DETECTION

- Identifiziert bislang unbekannte Bedrohungen
- Identifiziert unbekannte Anwendungen im Netzwerk
- Warnt vor Angriffen bei der Detektion von Datenfluss-Anomalien
- Besonders nützlich, wenn Endpunkt-Agenten nicht eingesetzt werden können

SECURITY OPERATIONS CENTER (SOC)

- Über 300 Sicherheitsexperten stehen in unseren Security Operations Centres (SOCs) für das 24/7 Monitoring und die Reaktion bereit
- Reaktionen mobilisieren und Empfehlungen aussprechen
- Standard-SOC-Services mit Advanced Threat Insights erweitern

PATCHING:
IHR ERSTER SCHUTZ VOR ANGRIFFEN

Ein einsatzkritisches System wie der mobile Landfunk (LMR) muss regelmäßig mit Software-Sicherheitsupdates versorgt werden (Patching). Allerdings führen nur 42 % der Unternehmen Patches durch. Dies ist unter anderem auf begrenzte Ressourcen und Fachkenntnisse zurückzuführen. Motorola Solutions bietet Ihnen entsprechende Lösungen.

42%
PATCHEN IHRE FUNKANLAGEN

ENTDECKEN & HERUNTERLADEN ▶ ANALYSIEREN & NACHHALTEN ▶ POSTEN & BEREITSTELLEN

BETRIEBSSYSTEM

VIRTUALISIERUNG

ANWENDUNG

ASTRO

WAVE RADIO GATEWAY

MOTOROLA SOLUTIONS

PATCH-PRÜFUNG UND -VALIDIERUNG

MCAFEE ANTIVIRUS SIGNATURES - WÖCHENTLICH
MICROSOFT WINDOWS - MONATLICH
WEITERE EXTERNE ANBIETER - QUARTALSWEISE

SICHERHEITSUPDATE-SERVICE
VOM KUNDEN SELBST INSTALLIERT

REMOTE-SICHERHEITSUPDATE
VERWALTETE PATCH-BEREITSTELLUNG

VOR ORT-SICHERHEITSUPDATE
LOKAL VERWALTETE PATCH-BEREITSTELLUNG

UNSERE LÖSUNG FÜR IHRE SICHERHEITSUPDATES (SUS)

SELBSTINSTALLATION

Wir bieten Ihnen ein umfassendes Patching-Angebot mit vorab getesteten Sicherheitsupdates, die auf der sicheren Website von Motorola Solutions verfügbar sind.

Heruntergeladen und installiert von: Kunde
Neugestartet von: Kunde

UPDATE VOR ORT

Unsere speziell geschulten MSI-Techniker führen die Patch-Updates und den Neustart Ihrer Server und Workstations vor Ort an Ihrem Standort durch.

Heruntergeladen und installiert von:
Motorola Solutions
Neugestartet von:
Kunde oder Motorola Solutions

FERNZUGRIFF

Unsere Techniker installieren die Sicherheitsupdates per Fernzugriff in Ihrem Funknetz.

Heruntergeladen und installiert von:
Motorola Solutions
Neugestartet von: Kunde

85%
DER GEZIELTEN ANGRIFFE KÖNNEN DURCH PATCHING VERHINDERT WERDEN

https://www.us-cert.gov/ncas/alerts/TA15-119A

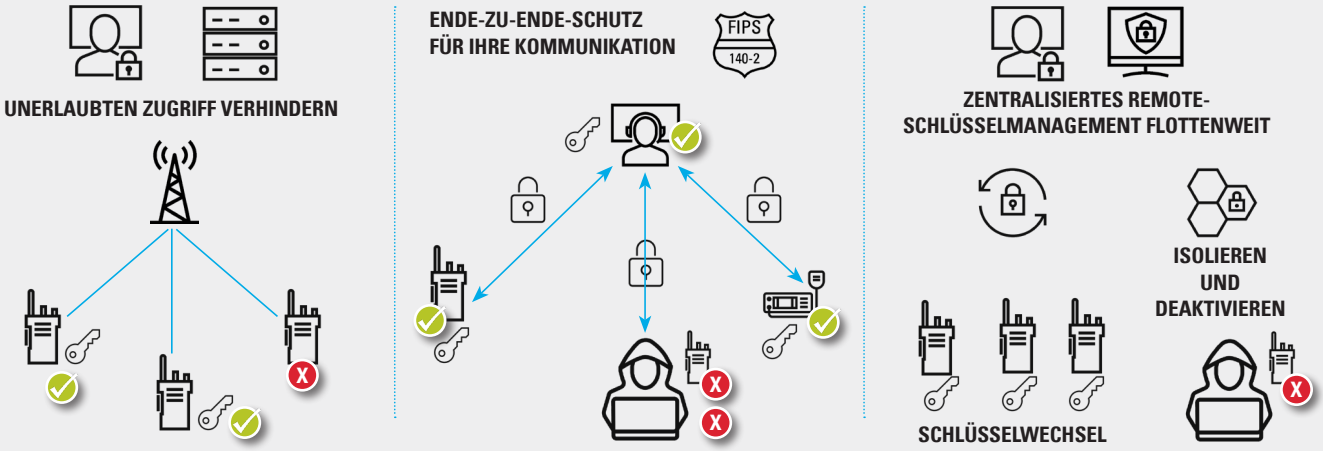
VOLLSTÄNDIGE KONTROLLE ÜBER IHR NETZWERK - SICHERESKALIERBARE UND BEWÄHRTE VERSCHLÜSSELUNGSLÖSUNGEN

Feindliche und proaktive Angriffe auf Ihr Netzwerk können jederzeit passieren – wir unterstützen Sie dabei, sich optimal vorzubereiten. Sichern Sie Ihre kritische Kommunikation, damit Sie schnell und einfach auf Bedrohungen reagieren können, ohne Ihre sensible Sprach- und Datenkommunikation zu gefährden.

Die Authentifizierung bietet eine Reihe von Sicherheitsoptionen. So ist sichergestellt, dass sich nur Geräte mit dem richtigen, aktuellen Sicherheitsschlüssel im System anmelden können. Per Ende-zu-Ende-Verschlüsselung wird Ihre Kommunikation verschlüsselt, bevor sie das Gerät verlässt, und nur der vorgesehene Empfänger kann sie entschlüsseln. Authentifizierung und Verschlüsselung sorgen dafür, dass Ihre Nachrichten und Daten nur von den vorgesehenen Empfängern gelesen werden können.

48%
DOKUMENTIEREN IHRE SICHERHEIT-SREGELN UND -VERFAHREN

AUTHENTIFIZIERUNG IHRER FUNKGERÄTE ▶ SPRACH- UND DATENVER-SCHLÜSSELUNG ▶ SCHLÜSSELVERWALTUNG



ZENTRALISIERTE ODER MANUELLE STEUERUNG DER VERSCHLÜSSELUNGSCODES. SO EINFACH KANN SCHLÜSSELVERWALTUNG SEIN. NUTZEN SIE DIE MÖGLICHKEITEN DER OVER-THE-AIR-ZUWEISUNG PER FERNZUGRIFF. AUTORISIERTE GERÄTE, DIE GEHACKT WURDEN, KÖNNEN SIE SOFORT BLOCKIEREN UND/ODER DEAKTIVIEREN.

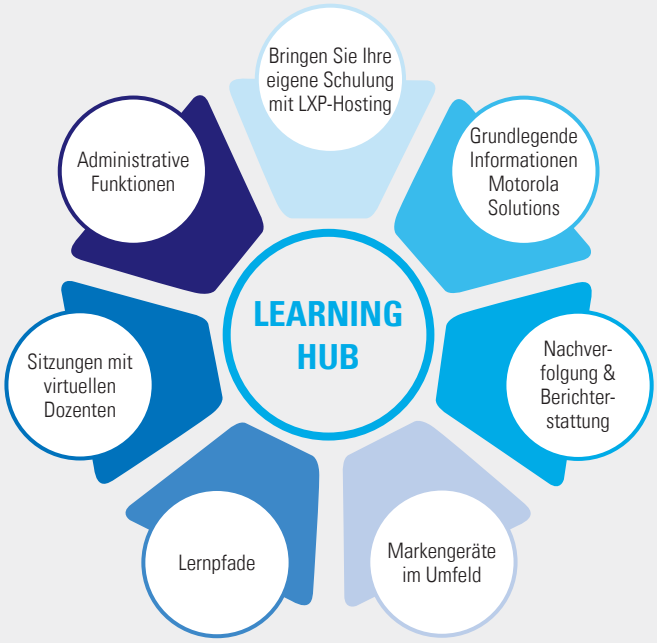
FACHWISSEN JEDERZEIT WEITERENTWICKELN STÄNDIGES LERNEN AN JEDEM ORT NUTZEN

Damit Sie Ihre Kenntnisse auf dem neuesten Stand halten können, bieten wir ein cloudbasiertes und zentral gehostetes Lernabonnement an, das Sie an Ihre eigenen Bedürfnisse anpassen können.

Über unser Cybersecurity Hub bieten wir sowohl formale als auch informelle Schulungen mit vielen verschiedenen Lernoptionen an, vom persönlich geleiteten Kurs bis zum Online-Format. So erhalten Sie zeitnahe, relevante und maßgeschneiderte Informationen und Kenntnisse im Bereich Cybersicherheit.

LERNPFADE

- Einführung in die Cybersicherheit
- Malware-Vorbeugung
- Cybersecurity: Bedrohungen und Angriffe aus dem Internet
- Auf Vorfälle reagieren
- Cyberkriminalitäts-Ermittlungen und Netzwerk-Forensik
- Schwachstellen-Prüfung



CYBER-GRUNDLAGEN

Überblick über die Terminologie der Cybersecurity-Profis, bewährte Praktiken zum Schutz Ihrer Daten

REAKTION AUF CYBERVORFÄLLE

Lernen Sie, wie Sie sich effektiv auf erfolgreiche Cyberangriffe vorbereiten, diese abwehren und darauf reagieren können.

MALWARE-PRÄVENTION

Erfahren Sie, was Malware ist und wie sie dazu verwendet werden kann, die Funktion Ihrer Geräte und Systeme zu stören.

ANATOMIE EINES CYBERANGRIFFS

Wir erklären Ihnen, wie ein Cyberangriff abläuft und wie unsere Experten mit Cyberangriffen umgehen.

VORBEREITUNG AUF CYBERANGRIFFE

Wir zeigen Ihnen, wie Sie sich effektiv auf einen Cyberangriff vorbereiten und diesen abwehren können. Anhand aktueller Beispiele für spezifische Angriffe erläutern wir Ihnen den Schaden und die Folgen eines Cyberangriffs.

IHR WEG IN DIE CYBERSICHERHEIT

Die Einführung und Umsetzung einer Cybersicherheitsstrategie wirft viele Fragen auf. Sollte Ihr Unternehmen nicht genügend interne Cybersecurity-Experten haben, stehen wir gerne als verlässlicher Partner an Ihrer Seite. Unsere Experten sind erfahrene Fachleute, die jederzeit zur Verfügung stehen, um Ihre Organisation dabei zu unterstützen, Bedrohungen aus dem Cyberspace besser zu erkennen und auf sie zu reagieren.

Für weitere Informationen besuchen Sie uns online unter
motorolasolutions.com/cybersecurity

Motorola Solutions Germany GmbH, Telco-Kreisel 1, 65510 Idstein, Deutschland.

MOTOROLA SOLUTIONS