computech

IT Sicherheit aus der Zukunft – für die Bedrohungen von Heute und Morgen.

Managed Security | Cloud & On-Premise

computech GmbH

computech-oberhausen.de

Neue Bedrohungen erfordern eine neue Form von Sicherheit.

Die fortschreitende Digitalisierung mit einer immer stärkeren Vernetzung, bedeutet mehr Freiheit und Flexibilität im Arbeitsalltag. Nicht länger sind wir strikt an die Arbeitsstätte und das lokale Firmennetzwerk gebunden, sondern arbeiten stattdessen vernetzt und digital – aus dem Home Office oder von unterwegs.

Doch diese neuen Freiheiten bedeuten auch neue Gefahren im Bereich der IT Sicherheit. Laut dem Bundesministerium für Sicherheit und Informationstechnik (BSI) sehen sich Unternehmen mit einem zunehmenden Anstieg an Cyber-Kriminalität in Form von Spionage, Erpressung oder Sabotage konfrontiert. Das gefährdet nicht nur die Geschäftskontinuität, sondern bedeutet auch einen erheblichen wirtschaftlichen Schaden durch Lösegeld oder Schutzgeld-Erpressung.

Umso mehr fordert die IT Infrastruktur von Morgen, dass heutige Sicherheitsmaßnahmen hinterfragt, neu gedacht und neu konzipiert werden. Wir unterstützen Sie dabei mit unseren **Managed Security Lösungen für Unternehmen**. 7 Tage die Woche, 24 Stunden am Tag. Um Schwachstellen und Angriffe zu vermeiden, noch bevor sie zum Problem für den Fortbestand Ihres Unternehmens werden.

144 Millionen

neue Schadprogramm-Varianten im Jahr 2021

223 Milliarden

Euro wirtschaftlicher Gesamtschaden

88% der Unternehmen

waren 2021 Opfer von Cyberangriffen

Kritische Bedrohungslage für KMU

Das BSI zeichnet in seinem jährlichen Bericht zur **Lage der IT Sicherheit in Deutschland** ein finsteres Bild hinsichtlich der Bedrohungslage im Bereich der Informationstechnologie. Alleine durch den rasanten Zuwachs an Ransomware, DDos Attacken mit Schweigegeld-, Lösegeld- oder Schutzgeld-Epressungen, klassifiziert das BSI die Bedrohungslage als angespannt bis kritisch. Besonders hervorgehoben wird im Bericht die Sonderstellung der rund 2,6 Mio. kleinen und mittelständischen Unternehmen (KMU), die durch teils mangelnde IT Sicherheitsinfrastruktur besonders anfällig gegenüber Cyber-Bedrohungen sind.

Das BSI rät daher explizit zu einem verstärkten Handeln und Ausbau des Engagements im Bereich IT Sicherheit, um langfristige wirtschaftliche Schäden zu vermeiden.

Quellen:
bitkom “Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr”
BSI Bericht “Die Lage der IT-Sicherheit in Deutschland”

Ein Schutz, der jede Minute dazulernt.

Managed Security mit Machine Learning.

Schützen Sie Ihr Unternehmen vor Malware, Exploits, Ransomware und digitaler Erpressung.

Eine zeitgemäße IT Sicherheitslösung sollte agieren statt nur zu reagieren. Mit Managed Security bieten für eine vollumfängliche Lösung für die Prävention und Härtung aller IT Systeme sowie erweiterte Erkennung, Reaktion und Risikoanalysen hinsichtlich potentieller Bedrohungen. Durch die Nutzung des weltweit besten und führenden Anbieters für Endpoint Security *Bitdefender**, schützen wir Ihre IT nicht nur vor klassischen Virenbedrohungen, sondern auch vor dateilosen, skriptbasierten Stealth-Attacken, die Systeme unerkannt infiltrieren können.

Die über 30 fortschrittlichen Abwehrtechnologien auf Basis von Machine Learning Algorithmen machen Managed Security dabei zu einer sich stets weiterentwickelnden Sicherheitslösung, die Ihre IT Umgebung flächendeckend vor heutigen wie auch zukünftig Bedrohungen schützt.

* Erstplatzierung AV-Comparatives Test 2021

Managed Security für Server

Gerade wenn Serversysteme als technisches Herzstück für die gemeinsame Arbeit im Unternehmen betrieben werden, sollten diese Systeme hinreichend geschützt sein, um Risiken und Bedrohungen frühzeitig zu erkennen und langfristige wirtschaftliche Schäden zu vermeiden. Mit **Managed Security Pro** und **Managed Security Ultra** helfen wir dabei. Mit bestem und noch besseren Schutz Ihrer Systeme.

ML Threat Detection
Cloudbasiertes und lokales maschinelles Lernen zur frühzeitigen Erkennung von Bedrohungen mit kontinuierlicher Selbstoptimierung.

Hyper Detect
Erweitertes Machine Learning Modell zum Blockieren von Hacker-Tools, dateilosen Angriffen und Zero-Day Schadsoftware.

Stealth Attack Detection & Defense
Frühzeitige Erkennung, Echtzeit Prävention sowie Abwehr von dateibasierten und skript-basierten Angriffen.

Cloud Sandbox Analyzer
Isolierung und Ausführung verdächtiger Dateien in einer geschlossenen, virtuellen Umgebung zur Verhaltensanalyse.

Network Attack Defense
Abwehr von Netzwerkangriffen wie Brute-Force Attacken und Netzwerk Exploits zum Eindringen in die Firmenumgebung.

Adanced Firewall & Web Filtering
Schutz aller Endpoints im Netzwerk vor unautorisierten Verbindungszugriffen und Blockieren spezifischer Web-Kategorien und Websites.

Wenn das Beste nicht gut genug ist.

Noch besserer Schutz mit Managed Security Ultra.

Managed Security Ultra für Server und Workstations

Der beste Schutz ist lückenlos und flächendeckend. Aus diesem Grund sollten stationäre wie auch mobile Endpoints nach den gleichen Standards geschützt werden wie die Serverinfrastruktur. Managed Security Pro und Managed Security Ultra stehen daher für Serversysteme, sowie auch als Add-On Lösung für die Arbeits-PCs Ihrer Mitarbeiter:innen zur Verfügung.

Für ein ganzheitliches Sicherheitskonzept ohne Schwachstellen.

ML Threat Detection
Cloudbasiertes und lokales maschinelles Lernen zur frühzeitigen Erkennung von Bedrohungen mit kontinuierlicher Selbstoptimierung.

Hyper Detect
Erweitertes Machine Learning Modell zum Blockieren von Hacker-Tools, dateilosen Angriffen und Zero-Day Schadsoftware.

Stealth Attack Detection & Defense
Frühzeitige Erkennung, Echtzeit Prävention sowie Abwehr von dateibasierten und skript-basierten Angriffen.

Cloud Sandbox Analyzer
Isolierung und Ausführung verdächtiger Dateien in einer geschlossenen, virtuellen Umgebung zur Verhaltensanalyse.

Network Attack Defense
Abwehr von Netzwerkangriffen wie Brute-Force Attacken und Netzwerk Exploits zum Eindringen in die Firmenumgebung.

Adanced Firewall & Web Filtering
Schutz aller Endpoints im Netzwerk vor unautorisierten Verbindungszugriffen und Blockieren spezifischer Web-Kategorien und Websites.

Endpoint Risk Management
Automatische Identifizierung und Analyse potentieller Sicherheitsschwachstellen.

EDR Visualization
Visualisierung von Angriffsketten (Kill Chain) zur Nachverfolgung potentieller Angriffe.

EDR Probing
Weiterführende Erkennung und Untersuchung von Sicherheitsvorfällen mit Kontextuntersuchung.

EDR Anomaly Detection
Erkennung potentieller Angriffe durch die Analyse von Abweichungen der normalen Verhaltensmuster.

EDR Isolation
Automatische Trennung infizierter und infiltrierter Endpoints vom Netzwerk zum Schutz weiterer Systeme.

Endpoint Detection and Response
Erweiterte Härtung und Schutz von Endpunkten im On-Premise oder Cloud Firmennetzwerk.

computech

Schützen Sie Ihre IT Infrastruktur mit Managed Security.

cloud@computech-oberhausen.de
+49 208 84 83 910