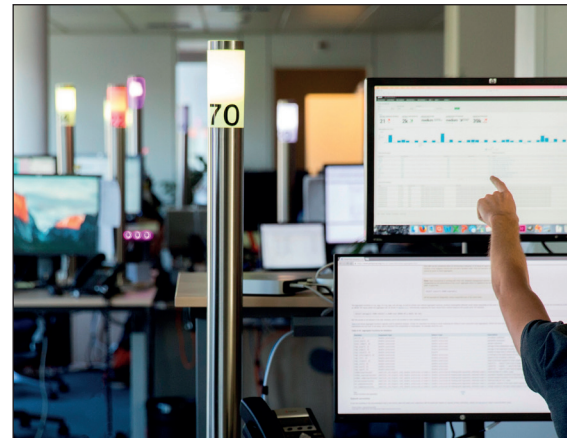


# Endpoint-Schutz mit Managed Security & Microsoft

Alle 40 Sekunden findet weltweit ein neuer Cyberangriff statt. Gleichzeitig bleibt die Personalsituation in der IT angespannt. Wie können Managed Security Services da helfen Engpässe zu vermeiden?



Über 65 % der Unternehmen weltweit verzeichneten in zwischen mindestens einen Cyberangriff, wobei E-Mail für die Verbreitung von 95 % aller Malware verantwortlich ist. Die angespannte Lage zwingt Unternehmen, mehr in Cyber Security zu investieren. Entsprechend planen auch die grossen Hersteller: allein Microsoft will in den nächsten 5 Jahren 20 Milliarden Dollar in die Weiterent-

wicklung ihrer Sicherheitssoftware stecken.

Jedoch ist es allein mit der Entwicklung von Software nicht getan. Jemand muss diese am Ende implementieren, bedienen und überwachen. Da die Pandemie aber die Digitalisierung aller Organisationen beschleunigt hat und diese noch mehr Fachkräfte verlangt, braucht es auch externe personelle Lösungen um Angriffe rechtzeitig erkennen und bekämpfen zu können.

## Mit MSS gegen Cyberkriminalität

Wer seine Cybersicherheit rasch ausbauen will, bei gleichzeitigem Personalmangel, setzt heute auf Managed Security Services (MSS), denn man schont die eigenen IT-Ressourcen und profitiert vom Know-how eines zertifizierten Partners. terreActive verfügt über 25 Jahre MSS-Erfahrung, ist Microsoft Silber Security Partner und überwacht von Aarau aus mit einem 80-köpfigen Team die IT-Infrastruktur zahlreicher Unternehmen. Urs Rufer, CEO, terreActive AG «Will man Bedrohungen aus dem Cyberspace begegnen, braucht es eine Kombination aus Beidem: Gute Software und verlässliche Services für den 7x24 Betrieb.»

## Endpoint Detection mit Microsoft

Besonderes Augenmerk legt terreActive auf den Schutz der Endpunkte, wo die meisten Angriffe geschehen. EDR, Endpoint Detection & Response, erlaubt einen schnellen Rollout und kann jederzeit

«Will man Bedrohungen aus dem Cyberspace begegnen, braucht es eine Kombination aus Beidem: Gute Software und verlässliche Services für den 7x24 Betrieb.»

Urs Rufer, CEO, terreActive AG

mit weiteren Lösungen (beispielsweise. SIEM) erweitert werden. Der Microsoft Defender for Endpoint bietet durch die Kombination von Erkennung,

Automation und dem Management von Schwachstellen mehr Sicherheit für Enduser. Mit MSS entscheidet der Kunde, wie schnell und wie stark er seine interne IT-Abteilung entlasten möchte, indem er aus einem modularen Servicekatalog seine benötigten Leistungen nach Belieben auswählt.

Neben den Services rund um Microsoft bietet terreActive noch weitere Managed Services an wie WAF, SIEM-Betrieb oder NDR Network Detection & Response.

DIE INHALTLICHE VERANTWORTUNG FÜR DEN ARTIKEL LIEGT BEI TERREACTIVE AG.

## SERVICE-BAUSTEINE FÜR CYBER SECURITY

### Threat Detection

Der Security Analyst vom MSS-Provider übernimmt die Klassifizierung von verschiedenen Sicherheitsvorfällen oder die Korrelierung von EDR-Alarmen mit weiteren Logquellen. Die tägliche Kontrolle der Kundeninfrastruktur ist hierbei ein Muss.

### Incident Response

Der Defender for Endpoint ist bereits mit Auto Investigation and Remediation ausgestattet. Das SOC-Team von terreActive empfielt dem Kunden Aufgaben, die automatisiert werden können und wählt den passenden Automatisierungsgrad. Aufgaben, die nicht automatisiert werden können, übernehmen die Security Engineers vom Incident Response Center in Aarau.

### Service Tuning

Hier liegt der Fokus auf der Reduzierung von Fehlalarmen innerhalb des Kundensystems. terreActive schärft die Erkennungsmechanismen des Microsoft Defenders durch die Klassifizierung von Alarmen, wodurch langfristig weniger Alarmmeldungen erzeugt werden. Durch dieses Tuning wird die Sicherheit kontinuierlich erhöht.

## JOBTIPP: IT-KARRIERE MIT 2 STANDBEINEN

Wenn du bereits über Know-how im Bereich Microsoft Security verfügst, mach den nächsten Schritt in einem Security Operations Center eines MS Security Partners. Im SOC sind spannende Cybervorfälle garantiert.

## KONTAKT

terreActive AG  
www.security.ch  
info@terreActive.ch  
062 834 00 55