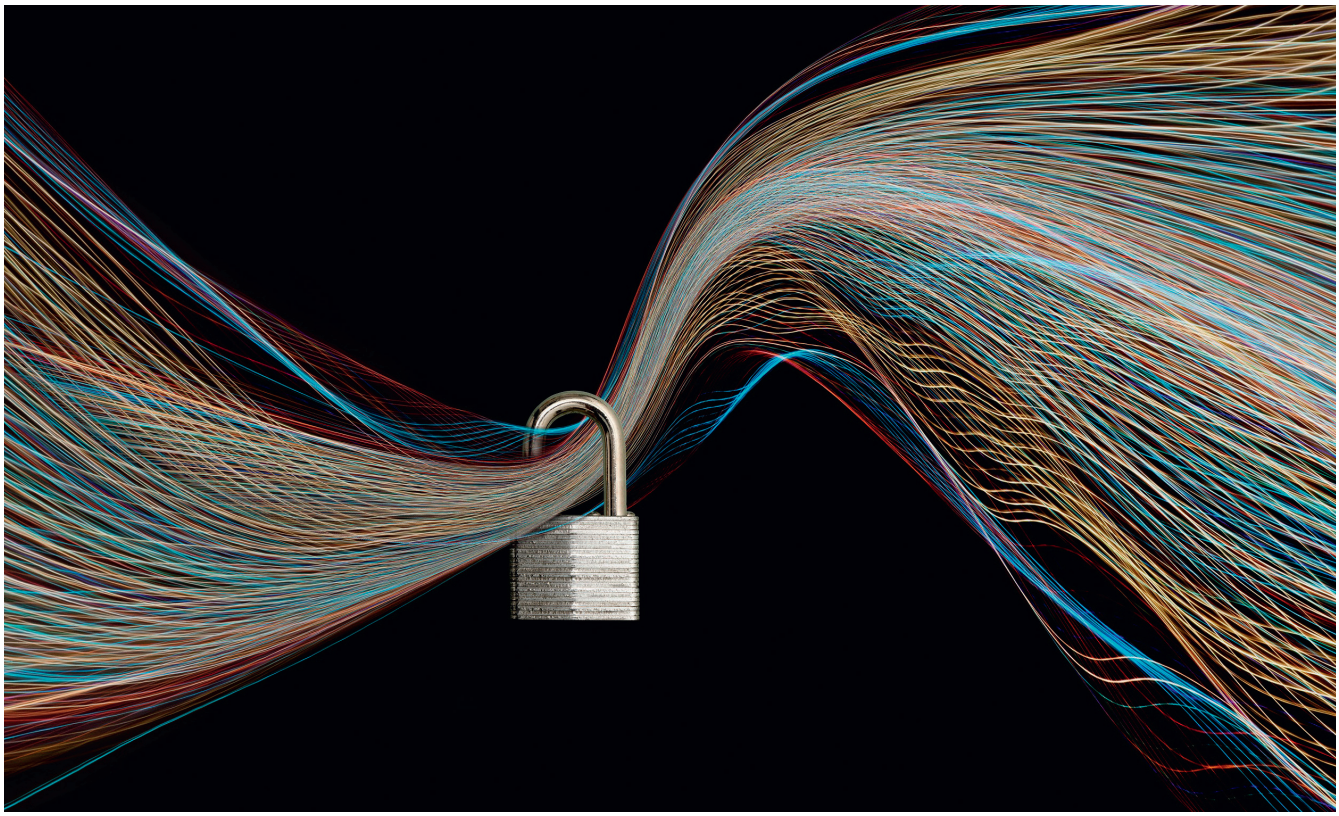

Prädiktive Sicherheit und Automatisierung

Die nächste Generation Security Operations Center | Der Erfolg der digitalen Revolution wird davon abhängen, wie schnell sich die Cybersicherheit entwickelt. Denn es gilt, den immer komplexeren, schnelleren und aggressiveren Bedrohungen effizient zu begegnen und digitale Innovationen zu schützen. Warum und wie lassen sich diese Anforderungen mit dem Ansatz der Prescriptive Security erfüllen?

PATRIK BENGTSSON, YANNICK RAGONNEAU

Bisher lag der Fokus in der Cybersicherheit auf der Erkennung und Überwachung der IT-Umgebung: Man wartete darauf, dass eine Sicherheitsverletzung eintrat. Dieser Ansatz kann zu schwerwiegenden Fehlern führen. Denn Cyberattacken können ihren Ursprung auch in nicht überwachten Umgebungen haben und dann ungestört bis zu den sensiblen Datenbeständen vordringen. Angriffe können Sicherheitsmassnahmen auf Basis eines solchen Ansatzes leicht umgehen, da er auf Annahmen und Korrelationsregeln basiert. Ein adäquates Reagieren auf eine sich verändernde Bedrohungslandschaft **(Bild 1)** ist so nicht möglich.

Die selbstadaptive Sicherheit

Entscheidend ist, wie Firmen Informationen aus hybriden Quellen nutzen, um sich gegen Cyberangriffe zu wappnen. Genau darum geht es bei Prescriptive Security. Der Blick auf die anderen gängigen Analysemethoden veranschaulicht, worin der Fortschritt besteht. So beschreibt deskriptive Analytik: Was ist passiert? Die diagnostische Analytik geht weiter: Warum ist es passiert? Und die prädiktive Analytik errechnet: Wie hoch ist die Wahrscheinlichkeit, dass es passiert? Die präskriptive Analytik baut auf diesen Methoden auf, um den nächsten Schritt zu gehen: Sie nutzt grosse Datenmengen und maschinelles Lernen. So lassen sich alle Daten, die in einer Firma selbst oder ausserhalb generiert werden, analysieren, Rundum-Sicherheit und Visibilität gewährleisten und potenzielle tote Winkel abdecken. Schliesslich definiert Prescriptive Security die nötigen Massnahmen, um die vorhergesagten Ergebnisse zu

Bilder: Atos, Getty, Gartner

erzielen und beschreibt die Auswirkungen jeder Entscheidung. So wird schnelles Handeln im Rahmen einer selbstadaptiven Sicherheit möglich.

Transformation der SOC

Security Operations Centers (SOC) schützen sowohl Geschäftsdaten als auch persönliche Kundendaten. Den Prescriptive-Ansatz in ein solches SOC zu implementieren, erfordert eine tiefgreifende Transformation. Wichtige Werkzeuge dafür sind die zentrale Nutzung von Big Data Analytics, maschinellem Lernen und Bedrohungsmodellen. So lässt sich die Cyberkriminalität eindämmen, indem Firmen mit Supercomputing aus historischen Daten lernen und dann entsprechende Algorithmen implementieren. Präskriptive Security Analytics integriert alle Schlüsselelemente in der Umgebung und nutzt Bedrohungsinformationen, die ausserhalb des Unternehmens gesammelt wurden (Surface Web, Dark und Deep Web usw.), um künftige Cyber-Angriffe zu blockieren **(Bild 2)**.

Die beste Option für Unternehmen ist es, proaktives Threat Hunting zu betreiben und die Schwachstellen in einer Umgebung zu identifizieren, bevor Cyberkriminelle ihnen zuvorkommen. Threat Intelligence soll dabei den Anspruch erfüllen, die ganze Angriffsfläche und alle Angriffsvektoren abzudecken. Durch die Integration von Threat Intelligence in das Prescriptive SOC ist die Bedrohungsaufklärung nicht mehr ein separater Prozess bei der Technologieüberwachung, der durch Alarmbulletins gesteuert wird. Er wird vielmehr zum integralen Bestandteil des SOC, bei dem die Informationen zur Aufklärung von Bedrohungen umsetzbare Risikobewertungen liefern und bislang unbekannte Bedrohungen erkennen, bevor diese die Firma erreichen. Zudem weist das Prescriptive SOC die Sicherheitskomponenten in der von ihm kontrollierten adaptiven Umgebung an, sich anzupassen und sich von Bedrohungen zu regenerieren. Diese Komponenten spüren Bedrohungen nicht nur auf (Threat Hunting), sondern beseitigen diese auch gleich.

Reaktionen automatisieren

Prescriptive Security erweitert die Grenzen eines dreidimensionalen Paradigmas – mit grösserer Erken-

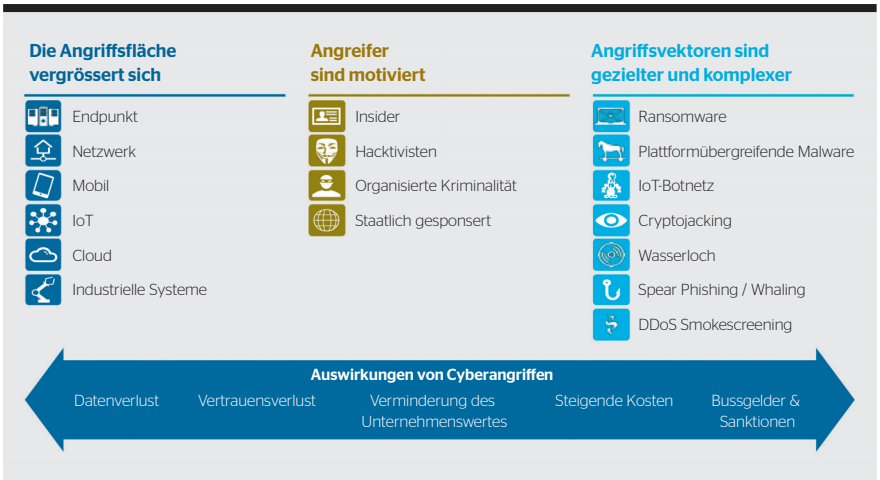

Bild 1 Die Bedrohungslandschaft entwickelt sich kontinuierlich.

nungsfläche, schnelleren Entscheidungen und kürzeren Reaktionszeiten. Werden Bedrohungen erkannt, gilt es sofort zu reagieren. Das präskriptive Sicherheitsmodell minimiert den Bedarf an menschlichem Eingreifen. Unternehmen bekämpfen auf diese Weise Bedrohungen nicht nur schneller, sondern analysieren auch deren Ursachen und verhindern erneute Angriffe in der Zukunft. Automatisierung setzt Ressourcen frei.

Unternehmen sollten sich bewusst machen, dass, wenn sie lediglich Tools für Big Data und Analytics einsetzen, nichts erreichen. Dies kann zum Beispiel in den bereits überlasteten SOCs unnötige Mehrarbeit verursachen.

Worauf es ankommt

Das Implementieren des präskriptiven Ansatzes legt mit der Datenerfassung die Basis, die beispielsweise beim Security-Operations-Modell von Atos folgendermassen funktioniert. Der Atos Data Lake stellt umfassende Kapazitäten zur Erfassung und Speicherung von Daten bereit. Zur Lösung gehört auch eine industrialisierte Analyse-Software-Suite. Damit lassen sich zudem Daten berechnen, verteilen und analysieren – validiert und in eine Appliance mit Hadoop-Verteilung integriert.

Erkennungs- und Bewertungsfunktionen sind in das Security Information and Event Management (SIEM) integriert. So kann das SOC Anomalien priorisieren und qualifizieren. Um Vorfälle effektiv zu bearbeiten und zu beheben, stehen Drill-Down-Funktionen zur Untersuchung der Anomalien mit genauen Kombinationen von Verhaltensweisen und Profilen zur Verfügung.

Durch das nahezu unbegrenzte Speichern von Protokollen und sicherheitsrelevanten Ereignissen ist es möglich, in historischen Daten nach neu entdeckten und charakterisierten Bedrohungen zu suchen. Das präskriptive Security Operations Center nutzt Data Lake Analytics, um kontinuierlich nach Indikatoren aus verschiedenen Quellen zu suchen. So können Anwender selbst lang andauernde Angriffe über Jahre hinweg verfolgen. Echtzeit-Hunting wird auch durch einen Data Exchange Layer ermöglicht, der neu erkannte Indikatoren verpackt und an die aktiven Sicherheitskomponenten im Netzwerk sendet. Damit lassen sich betroffene Systeme aufspüren und bearbeiten.

Visualisierte Bedrohung

Als Ergebnis eines präskriptiven Modells erhalten Sicherheitsanalysten eine visuelle Darstellung, mit der sich die relevanten Daten besser identifizieren lassen. Der rechtzeitige Zugriff auf vollständige und aggregierte Kontextdaten beschleunigt und erhöht die Genauigkeit der korrekten Einordnung von Ereignissen und reduziert falsche Fährten (False Positives und False Negatives) erheblich. Security-Compliance- und Risiko-Manager haben Zugriff auf Dashboards, welche die KPIs zum Sicherheitsstatus ihrer Umgebung anzeigen. So können sie die Wirksamkeit der implementierten Sicherheitskontrollen stets im Auge behalten.

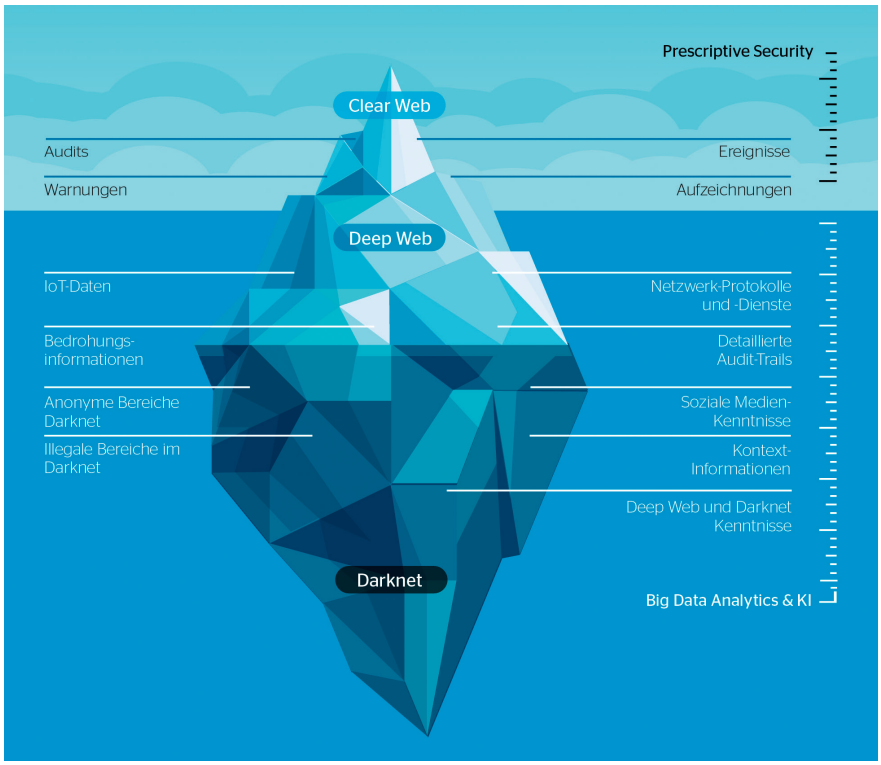

Bild 2 Die Art des Netzwerks bestimmt die erforderlichen Sicherheitsmassnahmen.

Ermittlungsanalysten erhalten aussagekräftiges Material für die Forensik. Dank Geopositionierung lassen sich die Erfahrungen in den entsprechenden Kontext setzen. So entsteht eine noch nie dagewesene Perspektive auf die örtliche Sicherheitslage, das Benutzerverhalten oder die Profilierung von Tätern.

Künftige Bedrohungen

Firmen benötigen heute ein flexibles Sicherheits-Framework, das herkömmliche mit neuen Sicherheitslösungen kombiniert. Dies verspricht das Implementieren des präskriptiven Modells in ein SOC, das sich auf analytische Muster konzentriert, um neue Bedrohungen zu identifizieren und Reaktionszeiten signifikant verkürzt. Methoden wie Threat Hunting, das Sammeln und Korrelieren von Bedrohungsdaten, maschinelles Lernen und Automatisierung von Reaktionen führen zu der Fähigkeit, Angriffe in Echtzeit zu neutralisieren und künftig gleichartige Sicherheitsverletzungen zu verhindern. Hier hilft Big Data Analytics, Angriffe schon in der Anfangsphase zu erkennen und schneller zu reagieren. Darüber hinaus lässt sich in einem Prescriptive SOC durch künstliche Intelligenz und automatische Reaktionen der Einsatz von Security-Experten optimieren, die sich auf komplexere Angriffe konzentrieren können. Prägend für die nächste SOC-Generation wird jedoch sein, dass sie prädiktive Sicherheit und Automatisierung mittels Supercomputing unter einen Hut bringt.

Autoren
Patrik Bengtsson ist Acting Head Cyber Security bei Atos.
→ Atos, Freilagerstrasse 28, 8047 Zürich
→ patrik.bengtsson@atos.net

Yannick Ragonneau ist Head Cyber Security bei Atos.
→ yannick.ragonneau@atos.net

RÉSUMÉ

Sécurité prédictive et automatisation

La prochaine génération de Security Operations Center

Aujourd'hui, les entreprises ont besoin d'une infrastructure de sécurité flexible qui combine les solutions traditionnelles à de nouvelles solutions basées sur la situation pour assurer une sécurité permanente. C'est ce que promet l'implémentation du modèle prescriptif dans un Security Operations Center (SOC), lequel se concentre sur un modèle analytique pour identifier de nouvelles menaces ainsi que pour réduire de manière significative le temps de réaction des contrôles de sécurité. Les méthodes comme le Threat Hunting, la collecte et la corrélation de données relatives aux menaces, l'apprentissage automatique et l'automatisation des réactions permettent de neutraliser les attaques en temps réel et d'éviter le même type de violations de la sécurité à l'avenir. Dans ce contexte, l'analyse des données au niveau du big data (Big Data Analytics) aide à détecter les attaques dès la phase initiale et à réagir plus rapidement. En même temps, les coûts liés à la sauvegarde et à la puissance de calcul sont moins élevés dans la mesure où 90 % des données ont moins de deux ans. Dans un SOC prescriptif, l'intelligence artificielle et les réactions automatiques permettent en outre l'optimisation de l'intervention des experts en sécurité, qui peuvent alors se concentrer sur des attaques plus complexes. Cependant, ce qui marquera la prochaine génération de SOC sera le fait qu'elle associe sécurité prédictive et automatisation au moyen de supercalculateurs. NO