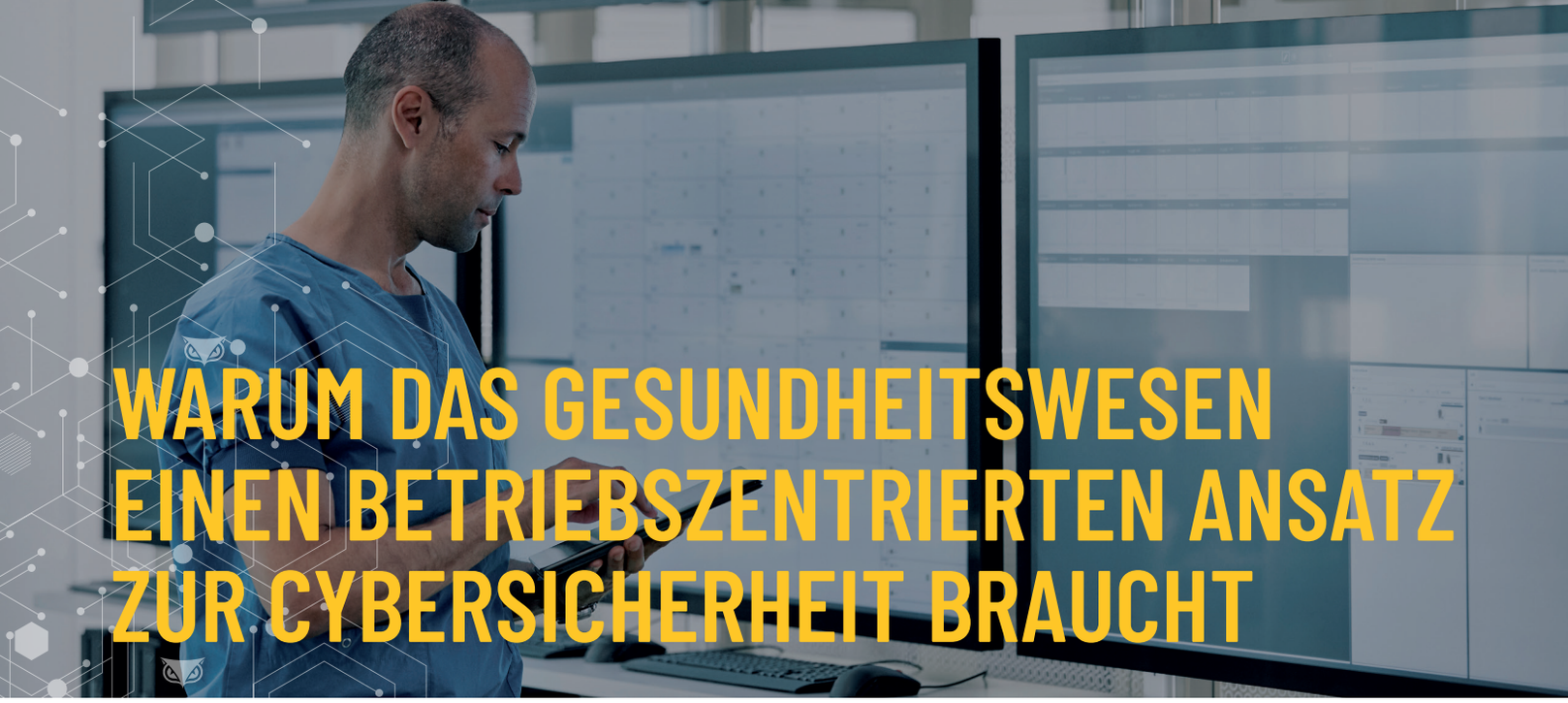

WARUM DAS GESUNDHEITSWESEN EINEN BETRIEBSZENTRIERTEN ANSATZ ZUR CYBERSICHERHEIT BRAUCHT

Das Gesundheitswesen bekommt im Moment deutlich mehr Aufmerksamkeit als sonst. COVID-19 hat wirtschaftliche und betriebliche Prozesse massiv beeinträchtigt, während sich gleichzeitig alle bemühen, die Pandemie unter Kontrolle zu bekommen.

Besonders das Gesundheitswesen ist in den Fokus von Cyberkriminellen gerückt, die versuchen, aus dem Druck in Zusammenhang mit der Pandemie Kapital zu schlagen.

GESUNDHEITSWESEN UNTER BESCHUSS

Während die Gesundheitsbranche um die Eindämmung der Pandemie ringt, nutzen Cyberkriminelle ihre Chance. Die teilweise unklare Situation und der wachsende Stresspegel im Gesundheitswesen machen es zu einem idealen Ziel für bösartige Operationen und Ransomware-Angriffe. Einrichtungen im Gesundheitswesen selbst, aber auch pharmazeutische Unternehmen und Forschungseinrichtungen sind vorrangige Ziele.

DEN GESAMTEN CYBERANGRIFF IM AUGE BEHALTEN

Effektive Cybersicherheit ist wie ein Puzzlespiel. Ein einziges Teil ergibt kein Gesamtbild.

Malops™ – kurz für Malicious Operations – umfassen eine Vielzahl von Taktiken und Techniken (Puzzleteile), die ein Gesamtbild ergeben. Mithilfe der Indicators of Behavior (IoBs) ist es möglich, verdächtige oder bösartige Aktivitäten schnell zu identifizieren. Gleichzeitig schafft man Transparenz, erhält den notwendigen Kontext und bekommt Informationen, um schon frühzeitig Maßnahmen zu ergreifen und zu reagieren.

Ein reaktives Cybersicherheitsmodell und das (meist vergebliche) Bemühen, eine überwältigende Anzahl von Alarmen zu bearbeiten, ist schlicht nicht effektiv genug, um diese Art aktueller Bedrohungen zu stoppen.

Ein operationszentrierter Sicherheitsansatz erlaubt es demgegenüber, Angriffe früher zu erkennen und schneller Abhilfe zu schaffen – lange bevor sie das Ausmaß schwerer Sicherheitsverletzungen erreichen. Weltweit versuchen Zehntausende von Unternehmen und Behörden, nach den SolarWinds- und HAFINUM-Angriffen wieder auf die Beine zu kommen. Monatelang waren die Angreifer in den Systemen unterschiedlicher Unternehmen aktiv. Und bei jeder dieser Aktivitäten haben sie Spuren ihrer Anwesenheit hinterlassen. Nur, dass die Beweise schnell in dem schier endlosen Strom nicht zueinander korrelierter Alarme untergegangen sind. Ohne den nötigen Kontext, um die einzelnen Angriffe richtig zuordnen zu können, blieb das Ausmaß der globalen Operation weitgehend unentdeckt. Komplexe Netzwerkinfrastrukturen mit einem alarmzentrierten, isolierten Ansatz zu schützen, schafft Cyberkriminellen einen großzügigen Spielraum, um tief in das Netzwerk einzudringen. Jeder Versuch, einen Angriff zu erkennen, nachzuverfolgen oder zu beseitigen, wird erschwert bis nahezu unmöglich gemacht. Alarmzentrierte Ansätze treiben Unternehmen in eine unerbittliche Spirale, weil sie nur Symptome bekämpfen, nicht aber die Ursache.

FAZIT

Ein operationszentrierter Ansatz ermöglicht es, einen Angriff von den Grundzügen bis hin zum eigentlichen Zugriff auf betroffene Endpunkte zu erfassen.

Wer den Zeitaufwand für das Erkennen und Beseitigen von Angriffen senken und Ressourcen für effektivere Sicherheitsinitiativen freischaufeln will, der kommt an diesem Ansatz nicht vorbei. Mit seiner Hilfe können Unternehmen den Spieß umdrehen und sich gegen zukünftige Bedrohungen wappnen. ■

Kontaktieren Sie uns am besten gleich, bevor Sie Opfer eines Cyberangriffs werden:
https://www.cybereason.com/de/

cybereason