concentrade
The Cybersecurity Company

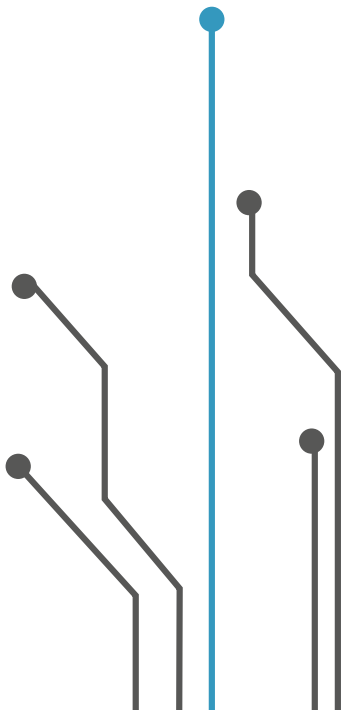
CASE STUDY

DECOYS UND BREADCRUMBS

INNOVATIVES SECURITY-KONZEPT ERHÖHT RESILIENZ VON BUSINESS-IT

bilsteingroup® »CYBERSENSE

Die ***bilstein group*** ist ein weltweit führender Anbieter im freien Ersatzteilmarkt. Der spezialisierte Lieferant und Hersteller bietet Reparaturlösungen für alle gängigen Fahrzeugtypen im Bereich der Personen- und Nutzkraftwagen. Nach der weltweiten Expansion passt das Unternehmen die historisch gewachsene IT-Infrastruktur mit seinem langjährigen IT-Dienstleister ***concentrade*** an. Angesichts der zunehmenden Anzahl von Cyberangriffen wurde die Infrastruktur zusätzlich durch eine Lösung zur Angriffserkennung ausgestattet, um die maximale Sicherheit zu gewährleisten. In enger Zusammenarbeit mit den Sicherheitsexperten von concentrade kam dabei die effiziente Lösung ***Cybersense Managed Breach Detection & Response*** zum Einsatz. Innerhalb von nur zwei Wochen ließ sich die Lösung zur Angriffserkennung über das gesamte interne Netzwerk ausrollen.



Der moderne Unternehmensalltag wird immer vernetzter, doch das erhöht auch die Risiken von Online-Attacken. „Üblicherweise sind Unternehmen mit klassischen Sicherheitssystemen gut geschützt", sagt Jens Albrecht, Geschäftsführer des Cybersecurity-Dienstleisters concentrade. „Allerdings werden die Attacken immer raffinierter. Einen hundertprozentigen Schutz kann es mit herkömmlichen Maßnahmen nicht geben", ergänzt Albrecht. „Darum raten wir unseren Kunden grundsätzlich zu einer zuverlässigen Angriffserkennung. Zu oft gelingt es Cyberkriminellen trotz aller Vorsichtsmaßnahmen, in Unternehmensnetze einzudringen." Zusätzlich können über Social Engineering und Spear-Phishing einzelne Mitarbeiter manipuliert und unwissentlich zu Komplizen werden – die sogenannte Insider-Bedrohung.

Laut dem Data Breach Investigations Report 2023 von Verizon gehen 83 Prozent der Sicherheitsverletzungen auf das Konto externer Akteure – mit meist finanziellen Motiven. Und 74 Prozent der Vorfälle wurden durch erfolgreiche Social-Engineering-Angriffe, Fehler, Missbrauch und andere menschliche Fehler ermöglicht. Wichtig ist daher ein umfassender Schutz des Firmennetzwerks. „Eine gute IT-Security verteidigt sich nicht nur nach außen, sondern verfügt auch über eine innere Wehrhaftigkeit", erklärt Sebastian Struwe, Geschäftsführer von Cybersense. „Die bilstein group ist sich der Gefahren bewusst und hat sich daher externe Hilfe bei uns geholt." Ende 2022 überzeugte Cybersense Managed Breach Detection & Response bereits mit einem ersten Proof-of-Concept. Daraufhin folgte ein Kickoff-Termin Anfang Dezember, an dem die technische Umgebung festgelegt wurde und eine intensive Sicherheitsberatung durch concentrade erfolgte. Die Cybersense-Lösung ist dank seines komplementären Ansatzes eine optimale Ergänzung zu klassischen Systemen der Angriffserkennung.

DECOY-SERVER KÖDERN
UNERWÜNSCHTE EINDRINGLINGE

Die IT-Abwehr von Unternehmen ist ständig unter Beschuss. Täglich suchen Hacker nach Schwachstellen, erhalten mithilfe von Phishing-Attacken oftmals Zugriff auf Accounts und übernehmen sie. „Unsere Lösung sorgt für eine effiziente Verteidigung, nachdem der Hacker die herkömmlichen Maßnahmen überwunden hat", erklärt Struwe. „Sie nutzt eine Art virtuelles Fallensystem, um Angreifer zeitnah aufzuspüren." Im Zentrum der Cybersense-Lösung bei der bilstein group stehen die Decoys. Dabei handelt es sich um Server, die keine produktive Aufgabe haben. Auf diese „Inseln der Ruhe" werden die Hacker durch sogenannte Breadcrumbs gelockt – für den Eindringling scheinbar wertvolle Informationen, wie zum Beispiel zusätzliche Accounts in der Anmeldeinformationsverwaltung von Windows. Sie sind in einem unauffälligen Muster über das gesamte Unternehmensnetz verteilt und werden „agentless" abgelegt.

Die Decoy-Server sind nicht von der restlichen Infrastruktur zu unterscheiden. Greift jemand darauf zu, kann die IT-Security sicher sein: Hier findet ein Angriff statt. „Beim Initial Access – dem ersten Zugriff auf einen kompromittierten Account – möchte sich der Angreifer weiter im infiltrierten Netz ausbreiten. Dafür sucht er bereits auf dem lokalen Computer nach weiteren Accounts", erläutert Struwe. „Durch unsere Breadcrumbs wird er aber beim ersten Auskundschaften auf eine falsche Spur gelenkt und landet in der Falle." Interaktion mit den Decoys werden sofort als Bedrohung gemeldet. Dadurch lassen sich zeitnah Verteidigungsmaßnahmen einleiten – beispielsweise das automatisierte Verschieben des kompromittierten Clients oder Servers in Quarantäne. Cybersense Managed Breach Detection & Response basiert auf einem komplementären Ansatz, der unabhängig von vorhandenen Systemen funktioniert und unterstützend wirken kann.

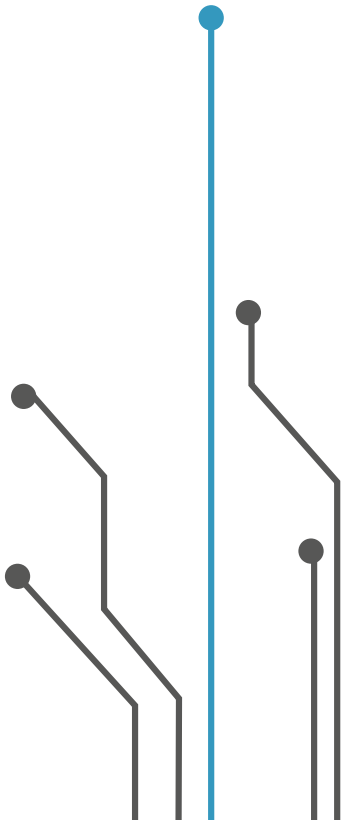
MANAGED SERVICE MIT HÖCHSTER TRANSPARENZ

Innerhalb von zwei Wochen wurde die Lösung umgesetzt und implementiert. Dabei stand die bilstein group in kontinuierlichem und engem Kontakt mit concentrade. „Uns war wichtig, die IT-Infrastruktur rechtzeitig vor Weihnachten abzusichern", sagt Olaf Fichtl, IT Operations Team Manager bei der bilstein group. „Denn gerade in dieser Zeit sind die Online-Attacken am häufigsten und am gefährlichsten. Unserer Erfahrung nach setzen Cyber-Kriminelle auf eine verspätete Reaktion während dieser beliebten Urlaubszeit." Dank des schlanken Decoy- und Breadcrumb-Konzepts von Cybersense ließ sich der enge Zeitplan problemlos einhalten. Und nach einer kurzen Einführungsschulung von zwei Stunden wussten die Mitarbeiter der bilstein group schnell, wie sie mit dem System umgehen müssen. Transparenz wird bei dem Managed Service großgeschrieben. „Unsere Kunden haben vollständige Admin-Rechte für das gesamte System und Zugriff auf sämtliche Auswertungen von Cybersense", ergänzt Struwe. „Auf Wunsch bieten wir unseren Kunden daher auch tiefergehende Schulungen an, sodass sie die genauen Zusammenhänge zwischen den Meldungen verstehen und die Daten korrekt lesen können." Keine Daten verlassen das Unternehmen, sie bleiben stets on-premise. In Bezug auf den Umgang mit geschäftskritischen und sensiblen Informationen ist das in vielen Branchen zusätzlich ein Vorteil – beispielsweise im öffentlichen Dienst oder in Kommunen.

FAZIT

Dank der umfassenden Betreuung durch concentrade ließ sich die Sicherheit der IT-Infrastruktur bei der bilstein group umfassend optimieren. Seit Ende 2022 schützt die Cybersense-Lösung als Managed Service. Das Verteidigungssystem wird vollständig von den IT-Experten von Cybersense verwaltet. „Das ist ein großer Vorteil gegenüber klassischen SIEM-Lösungen oder sogar einem Security Operations Center, da wir selbst kein zusätzliches Personal bereitstellen müssen“, so Fichtl von der bilstein group. „Unsere neue Sicherheitslösung meldet Bedrohungen zuverlässig und treffsicher. Wir sind absolut zufrieden mit den bisherigen Ergebnissen.“ Aufgrund der positiven Erfahrungen wurde der Dienst mittlerweile vom 10/5-Betrieb auf einen durchgängigen 24/7-Service erweitert.

Neben dem täglichen Betrieb stehen concentrade und Cybersense auch in Bezug auf die aktuelle Bedrohungslage beratend zur Seite. Aufgrund des verstärkten Aufkommens von Online-Attacken durch KI-gestützte Tools ist es wichtig, regelmäßig Bilanz zu ziehen und eventuell die Systeme anzupassen. „Wir freuen uns, dass wir der bilstein group bei der Absicherung ihrer IT-Umgebung helfen können“, resümiert Struwe. „Wichtig ist uns, keine Insellösung zu implementieren, sondern auch Anknüpfungspunkte für SIEM, EDR/XDR oder SOCs zu bieten. Die IT-Sicherheit des Kunden hat für uns oberste Priorität.“



concentrade.de