

Success Story: MBCC Group

IT-SICHERHEITSAUDITS UND NETZWERK- BASIERTE PENETRATIONSTESTS ZUR BEWERTUNG DER CYBER SECURITY

© iStock.com/NicoElNino

UNSERE KOMPETENZEN UND LÖSUNGEN

Das Fraunhofer IESE bietet Ihnen innovative Lösungen zur Überprüfung und Verbesserung Ihrer IT-Sicherheit.

- Unabhängige und neutrale Bewertung Ihrer IT-Sicherheitslage
- Ermittlung von Empfehlungen und Verbesserungspotenzialen für Ihre IT-Sicherheit
- Durchführung von netzwerkbasierter Penetrationstests
- Individuelle Überprüfung und Bewertung von IT-Systemen

UM WAS ES GEHT

Als global agierendes Unternehmen mit mehr als 7.500 Mitarbeitenden verteilt auf über 300 Standorte in mehr als 60 Ländern hat die MBCC Group das Fraunhofer IESE mit der Überprüfung verschiedener Standorte bzw. Tochtergesellschaften hinsichtlich ihrer Cyber Security sowie der Durchführung regelmäßiger globaler netzwerkbasierter Penetrationstests beauftragt.

Die **IT-Sicherheitsaudits** dienen der neutralen und unabhängigen Ermittlung des aktuell erreichten Grads an Cyber Security. Zudem sollten Verbesserungspotenziale identifiziert und aufgezeigt werden, um das erreichte Niveau an Cyber Security weiter zu verbessern. Das Fraunhofer IESE greift hier auf mehr als 20 Jahre Erfahrung im Bereich der IT-Sicherheitsaudits zurück. Die Themen- und Kompetenzfelder der IESE-Expert*innen reichen vom Endgeräteschutz (Endpoint Protection) über Netzwerk- und Internetanbindung, die Nutzung von Cloud-Lösungen bis hin zur Bewertung und sicheren Umsetzung von Konzepten wie Zero Trust. Die Global IT Security der MBCC Group hat in mehreren Projekten verschiedene Tochtergesellschaften in Südamerika und Asien durch das Fraunhofer IESE untersuchen und bewerten lassen.



Obwohl wir schon sehr viel im Bereich IT-Sicherheit investieren und umsetzen, erweist sich die Zusammenarbeit mit dem Fraunhofer IESE als großer Mehrwert für die MBCC Group. Besonders gefällt mir die sehr freundliche Atmosphäre bei den IT-Sicherheitsüberprüfungen, in welcher auch sehr konstruktive und offene Diskussionen zu Verbesserungsmaßnahmen Raum finden. Man hat weniger das Gefühl auditiert zu werden, sondern vielmehr das eines kollegialen Austauschs, bei dem aber dennoch die relevanten Sicherheitsanforderungen und deren Umsetzungsgrad diskutiert werden.



Dr. Manuel Rudolph
Director Global IT Security
MBCC Group



Die globalen **Penetrationstests** dienen der neutralen und unabhängigen Ermittlung des aktuellen Lagebilds von »außen«. Damit werden Schwachstellen und mögliche Einfallstore identifiziert, die externe Angreifer (Hacker) ausnutzen könnten. Das Fraunhofer IESE nutzt hierfür eine professionelle Scan-Umgebung, die selbst entwickelt wurde, sowie einschlägige, frei verfügbare Werkzeuge, die es ermöglichen, größere Mengen an Systemen in einem kurzen Zeitraum zu überprüfen. Die Überprüfungen finden regelmäßig statt, da solche Penetrationstests immer nur eine Momentaufnahme des aktuellen Lagebilds liefern und Änderungen der Infrastruktur oder neue Erkenntnisse über Schwachstellen entscheidende Kriterien für die Bewertung des Lagebilds sind.

DIE HERAUSFORDERUNG

Die MBCC Group besteht aus vielen Tochtergesellschaften. Die IT für fast alle dieser Gesellschaften wird cloudbasiert mit hochmodernen und innovativen IT-Sicherheitslösungen betrieben. Es gibt wenige Gesellschaften, die in diese cloudbasierte IT noch nicht integriert wurden und mit traditionelleren IT-Infrastrukturen (Legacy IT) betrieben werden. Unabhängig davon, ob es sich um Legacy-Systeme handelt, ob die IT über die Cloud verwaltet wird oder ob sich Standorte in der Migration befinden – die Cyber Security muss immer bewahrt und kontinuierlich verbessert werden.

Neben verschiedenen Webseiten zu den vielen Produkten, Marken und Gesellschaften der MBCC Group werden auch öffentlich erreichbare Systeme und Anwendungen angeboten, die von potenziellen Hackern als Eintrittspunkt genutzt werden könnten. Diese regelmäßig zu prüfen, zu bewerten und im Falle von Schwachstellen geeignete Gegenmaßnahmen einzuleiten, ist eine herausfordernde Aufgabe. Zur Überprüfung des erlangten Grads an Cyber Security und der Effektivität der Umsetzung ist eine unabhängige, unvoreingenommene und neutrale Bewertung von Vorteil, möglichst von nicht involvierten Expert*innen. Diese Funktion übernimmt das Fraunhofer IESE in dem Projekt mit der MBCC Group.

DIE UNTERSTÜTZUNG

Das Fraunhofer IESE unterstützt die MBCC Group seit 2021. Seitdem wurden verschiedene Gesellschaften im Rahmen von IT-Sicherheitsaudits unter die Lupe genommen. Dies umfasst teilwei-

se auch die Überprüfung von IT-Dienstleistern, um eine ganzheitliche Betrachtung der Cyber Security zu ermöglichen.

Als Forschungseinrichtung der Fraunhofer-Gesellschaft beschäftigt sich das Fraunhofer IESE mit etablierten und gängigen Lösungen, aber auch mit aktuellen und innovativen Trends im Bereich Cyber Security. Insbesondere dies war einer der Beweggründe dafür, dass die MBCC Group das Fraunhofer IESE als Partner für die kompetente und neutrale Bewertung der IT-Sicherheit ihrer IT-Systeme gewählt hat.

Das Fraunhofer IESE arbeitet dabei in drei Phasen: In der ersten Phase nimmt das Projektteam Kontakt zu dem zu überprüfenden Standort auf und fordert verschiedene Informationen und Dokumente an. Sobald diese vorliegen, werden sie gesichtet und geprüft. Nun werden bereits von »außen« durchführbare Prüfungen wie netzwerkbasierte Penetrationstests oder manuelle Prüfungen von extern erreichbaren Diensten (z. B. der Webseite) durchgeführt. In der zweiten Phase erfolgt die Detailprüfung des Standorts remote oder vor Ort. Hierbei werden Systeme untersucht, Konfigurationen im Detail besprochen, Stichproben genommen und Prüfungen gemeinsam mit den IT-Verantwortlichen der Standorte durchgeführt. Die Befunde dokumentiert das IESE in einem Bericht und übermittelt sie zur weiteren Bearbeitung an das Unternehmen. In der dritten, optionalen Phase erfolgt eine Nachprüfung, inwieweit die ermittelten Befunde zufriedenstellend beseitigt wurden. Nach diesem Schema gehen die Expert*innen des IESE auch bei den IT-Sicherheitsaudits mit der MBCC Group vor.

Begleitend zu dieser Maßnahme erfolgen netzwerkbasierte Penetrationstests. Hierzu werden ausgewählte Systeme der MBCC Group durch das Fraunhofer IESE auf Schwachstellen untersucht. Die Expert*innen setzen hierbei auf eine Kombination aus automatisierten Prüfläufen und einer nachgelagerten intensiveren manuellen Prüfung. Schlussendlich geht es um die Ermittlung von Schwachstellen, die durch externe Angreifer missbraucht werden könnten. Das Fraunhofer IESE orientiert sich bei der Vorgehensweise an gängigen Empfehlungen und untergliedert die Arbeiten in die Schritte »Scoping«, »Testing« und »Reporting«. Beim »Scoping«

werden die Erwartungshaltung, das Angreifermodell, die Rahmenbedingungen wie Prüfzeiten und die Prüfobjekte sowie Tiefe und Aggressivität der Prüfung festgelegt. Beim »Testing« führt das Projektteam die automatisierten und manuellen Prüfungen durch, bewertet sie und bereitet sie so auf, dass die Befunde im Arbeitsschritt »Reporting« dokumentiert werden können. Bei kritischen Befunden erfolgt eine direkte Benachrichtigung, um einem Zeitverzug entgegenzuwirken.

Die Kombination aus IT-Sicherheitsaudits und flankierenden Penetrationstests unterstützt die MBCC Group bei einer ganzheitlichen Betrachtung ihrer Cyber Security.

DAS ERGEBNIS

Im Rahmen der IT-Sicherheitsaudits erhält die MBCC Group vom Fraunhofer IESE eine unabhängige, unvoreingenommene und neutrale Bewertung der aktuellen IT-Sicherheitslage der untersuchten Tochtergesellschaften in dokumentierter Form. Dieser Bericht umfasst neben der Zusammenfassung der ermittelten Befunde auch Empfehlungen und Maßnahmen, welche die Cyber Security der MBCC Group weiter verbessern und erhöhen können. Die Ergebnisse werden außerdem mit den lokalen, regionalen und globalen IT Verantwortlichen innerhalb der MBCC Group persönlich besprochen und diskutiert.

Als Ergebnis der netzwerkbasieren Penetrationstests erhält die MBCC Group auch einen Bericht vom Fraunhofer IESE, der die Durchführung der Testläufe und die ermittelten Befunde dokumentiert. Der Bericht umfasst ebenso eine Zusammenfassung der Ergebnisse und weiterführende Detailinformationen zu den Befunden. Da es sich hierbei um regelmäßige Überprüfungen der größtenteils gleichen Prüfobjekte handelt, werden in dem Bericht die aktuellen Ergebnisse mit den vorherigen Befunden verglichen. Dadurch kann einerseits die Effektivität der getroffenen Maßnahmen zur Behebung der Schwachstellen bestätigt werden und andererseits können nicht beseitigte sowie neu hinzugekommene Schwachstellen dargestellt werden.

Beide Berichte können zum einen als Nachweis für ein IT-Sicherheitsaudit herangezogen werden, zum anderen stellen sie die Ausgangslage zur Planung von Maßnahmen zur Verbesserung der Cyber Security dar.

Unternehmensprofil MBCC Group

Branche: Bauchemie

Sitz: Mannheim

Anzahl Mitarbeiter: 7.500

Projekt durchgeführt: 2021 und 2022

Kontakt

Christian Jung
Department Head Security Engineering
Telefon +49 631 6800-2146
christian.jung@iese.fraunhofer.de

Andreas Eitel
Expert »Cyber Security«
Telefon +49 631 6800-2291
andreas.eitel@iese.fraunhofer.de

www.iese.fraunhofer.de

