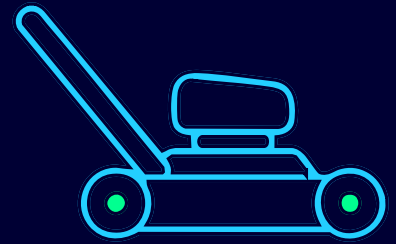


# XM Cyber und STIHL: Ein globales Erbe durch digitale Souveränität sichern



## Die Herausforderung

ein Jahrhundert der Innovation durch kontinuierliche Sicherheit schützen

STIHL ist ein in dritter Generation inhabergeführtes Familienunternehmen mit einer hundertjährigen Innovationstradition.

Mit zunehmender Vernetzung und Digitalisierung seiner Betriebsabläufe hat das Unternehmen frühzeitig erkannt, dass proaktive Cybersicherheit für den Schutz seiner Daten, seines Betriebs und seiner Reputation von entscheidender Bedeutung ist. Eine der Stärken des Unternehmens, so der Vorstandsvorsitzende Dr. Nikolas Stihl, ist es seit jeher, Risiken zu antizipieren, bevor sie auftauchen:

„Wer sich umhört und die technologischen Entwicklungen im Bereich Cyberkriminalität verfolgt, weiß, dass Unternehmen gezielt Vorsorge treffen müssen. Weil das von Anfang an unsere Herangehensweise war, sind wir bisher – trotz zahlreicher Angriffsversuche – ungeschoren davon gekommen.“

Diese Philosophie leitete STIHL beim nächsten Schritt. Das Führungsteam war bestrebt, seine schnell wachsende globale Infrastruktur abzusichern und gleichzeitig die volle Kontrolle über Daten, Systeme und Prozesse zu behalten. Das Unternehmen benötigte eine Lösung, die eine kontinuierliche Transparenz, klare Prioritäten für die Behebung und einen Echtzeitschutz bietet und gleichzeitig die strengen europäischen Datenschutzstandards erfüllt.

**STIHL®**

STIHL, ein weltweit führender Hersteller von Motorgeräten für die Forst- und Landwirtschaft sowie für den Garten- und Landschaftsbau, nutzt XM Cyber, das in der sicheren europäischen Cloud von STACKIT ausgeführt wird, um seine globalen Aktivitäten zu schützen, seine digitale Unabhängigkeit zu wahren und den sich entwickelnden Cyber-Bedrohungen einen Schritt voraus zu sein.

## Die Lösung

eine proaktive, souveräne Sicherheitsgrundlage

Vor dem Wechsel zu XM Cyber verfügte STIHL bereits über ein gut funktionierendes Sicherheitssystem, das jedoch nach der älteren Methode arbeitete, jeden einzelnen Angriff zu verhindern. Dr. Stihl erläutert, was sie überzeugte:

„Überzeugt hat uns bei XM Cyber der wirklich neue und innovative Ansatz: Einbrüche sind unvermeidlich. Doch die Folgen eines Einbruchs können beherrscht und begrenzt werden.“

STIHL entschied sich für XM Cyber, um die Transparenz und Kontrolle in seiner globalen Umgebung zu verbessern. Die Plattform, die in der souveränen europäischen Cloud von STACKIT ausgeführt wird, bildet kontinuierlich Risiken und Angriffspfade ab und hilft dem Unternehmen, Risiken zu lokalisieren und zu reduzieren, bevor sie den Betrieb beeinträchtigen können.

Wie Dr. Stihl feststellte, ermöglicht die Plattform seinem Unternehmen, seine Ressourcen auf die kritischsten Risiken zu konzentrieren:

„XM Cyber ermöglicht es uns, Schwachstellen nicht nur zu identifizieren, sondern auch zu priorisieren. So kennen wir die größten Risiken für unsere Geschäftsprozesse und können gezielt gegensteuern.“

XM Cyber unterstützt STIHL dabei, abzubilden, wie aus kleinen Schwachstellen Angriffspfade entstehen können, die zu kritischen Assets führen. Die Digital-Twin-Funktionalität der Plattform ermöglicht es STIHL zu validieren, was in seiner Umgebung wirklich ausgenutzt werden kann, ohne riskante Payloads auszuführen oder Systeme zu stören. Dies schließt blinde Flecken in der gesamten hybriden Infrastruktur aus und hilft den Sicherheits- und Betriebsteams von STIHL, sich auf die potenziellen geschäftlichen Auswirkungen von Gefährdungen und die besten Maßnahmen auszurichten.

Die Implementierung von XM Cyber verlief reibungslos und schnell. Die Plattform verschaffte STIHL schnell vollständige Transparenz und klare Anleitungen, wo zu handeln ist, und half dem IT-Team dabei, Risiken zu reduzieren und den Betrieb ohne Unterbrechung am Laufen zu halten. Dr. Stihl betonte den kooperativen Ansatz:

„Von Beginn an pflegen wir engen Kontakt zu den Spezialisten von XM Cyber in Israel, die uns beratend unterstützen.“

## Vorteile und Ergebnisse

### Sichtbarkeit, Belastbarkeit und Kontinuität

XM Cyber bietet STIHL eine konsolidierte Echtzeitansicht seiner digitalen Umgebung und die Möglichkeit zu handeln, bevor Bedrohungen eskalieren können. Die Analyse des Angriffspfads hebt nun die wenigen Korrekturschritte hervor, die viele Risiken gleichzeitig neutralisieren und die betriebliche Effizienz teamübergreifend erheblich verbessern. Mit stärkerer Belastbarkeit und größerer Zuversicht über alle Standorte und Systeme hinweg stellte Dr. Stihl fest, dass das operative Geschäft seines Unternehmens bemerkenswert stabil geblieben ist:

„In Zeiten, in denen es Vorfälle in vielen renommierten Unternehmen gab, haben wir keine Unterbrechung unseres Geschäftsbetriebs hinnehmen müssen.“

Diese kontinuierliche, angreiferbewusste Sichtbarkeit gibt STIHL die Voraussicht, um Schwachstellen frühzeitig zu erkennen und zu bestätigen, dass jede Fehlerbehebung die allgemeine Sicherheitslage des Unternehmens stärkt. Heute weiß STIHL, wie Angriffe ablaufen können, und nutzt diese Erkenntnisse, um seine Innovationen zu schützen, Systeme am Laufen zu halten und das Vertrauen in sein globales Netzwerk aufrechtzuerhalten.

## Empfehlung und Ausblick

### zukunftsichernde Risikosteuerung

STIHL's Partnerschaft mit XM Cyber spiegelt die strategische Verschiebung des Unternehmens in Richtung wirkungsorientierter Sicherheit wider. Das Unternehmen erkennt, dass Eingriffe zwar vorkommen können, die Folgen jedoch durch intelligente Vorbeugung, Behebung und schnelle Reaktion gesteuert und minimiert werden können. Dr. Stihl erläuterte, dass es letztlich nicht darum geht, alle Risiken zu eliminieren, sondern ihre Auswirkungen einzudämmen.

Digitale Souveränität bedeutet für STIHL, die Kontrolle über seine Daten, Systeme und Technik zu behalten. Mit XM Cyber kann das Unternehmen seine digitalen Plattformen zu seinen eigenen Bedingungen weiterentwickeln und gleichzeitig die sichere Grundlage für Innovation und globales Wachstum schützen.



**Kontinuierliche  
Transparenz über  
globale Systeme**



**Risikofrüherkennung  
und -priorisierung über  
Angriffspfade**



**Einhaltung europäischer  
Datenschutzstandards**



**Reibungsloser Einsatz  
ohne  
Betriebsunterbrechung**



**Stabilität und  
Entscheidungssicherheit  
gestärkt**