Gewappnet sein im Cyberkrieg: Blue Shield hat KI-Defensivwaffe

Der SolarWinds-Hack im Dezember des Vorjahres ist der größte Hackerangriff der US-Geschichte „und definitiv ein Game-Changer, dessen Folgen sich noch nicht abschätzen lassen“, sagt der Cyber-Security-Spezialist Avi Kravitz, seit Anfang 2020 im Expertenbeirat der Blue Shield Security GmbH mit Sitz in Linz-Leonding.

Mit dem Beginn des Ukrainekriegs haben sich die Cyberangriffe potenziert. Es bedarf einer Defensivwaffe, die neuartige Cyberbedrohungen erkennen und abwehren kann. Blue Shield hat mit dem Blue Shield Umbrella eine derartige Defensivwaffe entwickelt und ständig weiterentwickelt, sodass mit den neuesten Methoden der Künstlichen Intelligenz ein System auf White List Basis entwickelt wurde, das vollkommen neue Bedrohungen in Echtzeit erkennen kann. Eine Weltneuheit im Bereich der DNS Threat Intelligence. Made in Austria.

Der SolarWinds-Hack im Dezember wurde bereits ausführlich erforscht: Betroffen waren mehr als 18.000 Unternehmen und Organisationen weltweit, welche die Software des texanischen Netzwerkmanagement-Spezialisten SolarWinds verwenden. Hinter dieser raffinierten Attacke wird eine geballte Macht von 1.000 Programmierern vermutet – eine Attacke, die in mehreren Stufen abgelaufen ist. Motto: Wer SolarWinds hackt, hackt auch seine Kunden. Und die Kunden der Kunden. Einem Bericht des „Wall Street Journal“ zufolge, hatten 30 Prozent der angegriffenen Unternehmen keine direkte Verbindung zu SolarWinds. Alles begann Monate vorher mit einem präparierten Update der SolarWinds-Software namens „Orion“. Mit dieser Installation schufen sich die Hacker eine Hintertür ins jeweilige System.

Die betroffenen Unternehmen sind teilweise das Who‘s Who der Technologie-Giganten mit fortgeschrittenem Sicherheitsbewusstsein. Und dieses Beispiel veranschaulicht hier deutlich: Wir benötigen bessere Schutz- und Detektionsmöglichkeiten. Die Angreifer waren etwa neun Monate aktiv, bevor es irgendjemand (durch Zufall!) gemerkt hat! Die Angreifer seien mindestens zwei Schritte voraus.

Warum Zero Day Prävention

Es bedarf daher neuer Lösungen und Konzepte, um solche Cyberattacken systematisch erkennen zu können. Und es wird ein IT Security-System benötigt, das schlauer ist als die Angreifer – oder eines, das ein Eindringen von Schadsoftware von vornherein verhindert. Wie es geht, zeigte der heimische Anbieter Blue Shield Security, der mit dem auf künstliche Intelligenz basierten IT Security-System „Blue Shield Umbrella“ alle seine Kunden vor diesem Angriff schützen konnte.

Warum Blue Shield Umbrella sicher ist

„Während andere IT Security Lösungen meist mit einem Blacklist-basierten Ansatz arbeiten, der aber voraussetzt, dass der Schädling bereits bekannt ist, verfolgen wir einen gänzlich anderen Ansatz. Blue Shield Umbrella ist der erste auf KI basierte WhiteList- bzw. AllowList-DNS-Filter der Welt, der die Schadsoftware erst gar nicht ins System lässt und somit ein Infektionsrisiko von Anfang an ausschließt“, sagt Avi Kravitz. Der Cyber-Security-Experte ist davon überzeugt, dass dieser Angriff durch Blue Shield Umbrella hätte verhindert werden können – weltweit.

Über Blue-Shield

Das Blue-Shield-Headquarter mit mehr als 30 Beschäftigten im Bereich Forschung und Entwicklung befindet sich in Leonding bei Linz. Der seit 2015 in Österreich entwickelte Blue Shield Umbrella ist ein cloudbasiertes System und der weltweit einzige Whitelist-/Allowlist-Filter auf Basis künstlicher Intelligenz.

BlueShield