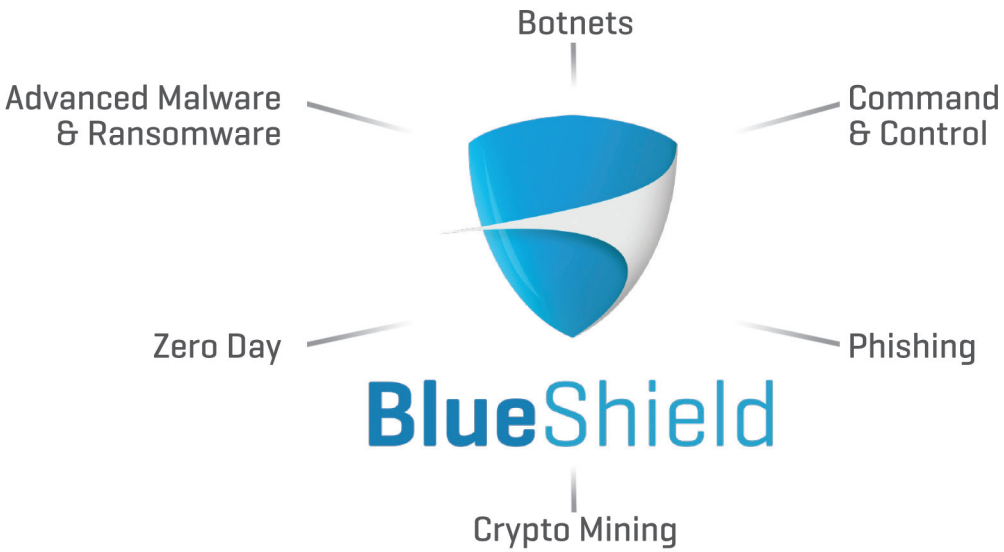
11.2020

CLOSING THE GAP BETWEEN 0-DAYS AND SIGNATURES POWERED BY BLUE SHIELD UMBRELLA

BLUE SHIELD UMBRELLA

- ist ein **cloudbasiertes System** aus Österreich
- Einziger auf KI-basierter Whitelist/Allowlist Filter am Markt
- **DNS-Filtering bereits vor Eindringen** in das Netzwerk
- Clients für alle **mobilen Plattformen**
- Ausschließlich Blockaden werden protokolliert und für 30 Tage im Dashboard sichtbar gemacht
- **Zero Day Prevention**
- Vorausschauender und **selbstlernender Schutz gegen neue Bedrohungen**
- Keine Signaturen oder Blacklists/ Denylists
- Alle **Prüfungen erfolgen in Echtzeit**
- **100% DSGVO-konform**

BLUE SHIELD UMBRELLA SCHÜTZT VOR



BEREITS UNTER UNSEREM SCHUTZSCHILD:

Banner · Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie · BBT · Hofburg Vienna · JKU Johannes Kepler University Linz · Land Kärnten · Kremsmüller Industrieanlagenbau · Medienhaus Wimmer · Ölz Der Meisterbäcker · Spitz · Vinzenz Gruppe · VKB-Bank · westbahn · Wiener Städtische

Blue Shield Security GmbH | Kornstraße 7A | 4060 Leonding | AUSTRIA | **www.blue-shield.at**

11.2020

CLOSING THE GAP BETWEEN 0-DAYS AND SIGNATURES POWERED BY BLUE SHIELD UMBRELLA

BLUE SHIELD FACTS & FIGURES

- Gründung 2015 (auf Basis F&E Tätigkeiten seit 2013)
- Eigentümergeführtes Unternehmen (Made in Austria)
- Globales Netzwerk
  Verarbeitung, Intelligenz und Reporting, garantiert in heimischen Rechenzentren
- Über 30 aktive F&E Mitarbeiter
- Weltweite Kooperationen im Bereich Forschung & Entwicklung
- Nur blockierte Anfragen werden protokolliert und nach 30 Tagen unwiderruflich gelöscht
- Zusätzlicher Schutz für alle mobilen Endgeräte
- Einziger Echtzeit-Whitelist/ Allowlist-Schutz

DIE TECHNIK DAHINTER

Eigene Spiegelung der Root-Server
Auf einer sogenannten „WhiteList/ AllowList" Root-Nameserver-Basis wird schon vorsortiert, bevor eine Domain in unser eigenes DNS-System aufgenommen wird. Zu dieser Bewertung, ob eine Domain auf der Blue Shield Umbrella Plattform aufgenommen und laufend überwacht wird, kommen speziell entwickelte Algorithmen, eigene Crawler und Künstliche Intelligenz auf Basis unserer eigenen PassiveDNS/ IP Datenbasis, welche seit 2013 analysiert und stetig mit weltweit öffentlichen Hybrid-Sandboxen erweitert wird.
Jeglicher Web Code wird auf schadhafte Software gescannt und auch weiterführende Links werden geprüft, z.B. für CDN[AK1] , Forum Links usw. - dadurch setzen wir im Bereich ZeroDay Prävention neue Maßstäbe.

Realtime Prevention
Dabei werden keine Ergebnisse gespeichert, sondern bei jedem Aufruf in Echtzeit die Verbindungs- und Metadaten des Zieles geprüft und mit Algorithmen unter Verwendung historischer Daten bewertet, ob das aktuelle Verhalten gut oder schlecht ist.

Sollte sich eine Infrastruktur drastisch ändern, sodass die historischen Daten nicht mehr zum aktuellen Verhalten passen, wird die Domain bis zur neuen Erstellung eines aktualisierten Profils gesperrt. Dieser Prozess passiert automatisiert im Hintergrund.

Code-Scans per KI im Hintergrund
Parallel laufen für die aufgerufenen Domains im Hintergrund Code Scans auf Basis des neuen mathematischen Algorithmus inklusive der speziell entwickelten Sandbox, um auch neben den Verbindungsdaten sofort zu erkennen, wenn sich ein Code bösartig verändert. Diese Information wird laufend herangezogen um festzustellen, ob die gewünschte Domain auf unseren Klonen der Root Nameserver weiterhin anerkannt wird.

Unbekanntes wird blockiert
Webserver, Domains, IPs und Authoritative Server, welche der BSU nicht kennt, werden zunächst blockiert und vom System automatisiert im Hintergrund überprüft, bevor sie freigegeben werden.

Während dieser Zeit analysiert und lernt unser System über das neue Ziel:
· Verbindungsverhalten
· Code Bewertung inkl. versteckter Unterverzeichnisse
· Jeglicher sonstige Traffic
· IP Reputation
· Alternative Nameserver Reputation
Zusätzlich kommt PassiveDNS/ IP Learning zum Einsatz
· Welche Domains/ IP's zeigen auf das Ziel, sind diese schon aufgefallen
· Owner der Domain inkl. seiner Historie
· Authoritative Nameserver

Laufende Bewertung & Überprüfung der Whitelist/ Allowlist
Nur wenn alle Kriterien positiv bewertet werden können, wird eine Domain in die eigenen Root Nameserver aufgenommen und dann zusätzlich durch Realtime Prevention und Code-Scans per KI überprüft.

Daten & Fakten
Aktuell blockieren wir alle Domains von mehr als 4000 Authoritative Nameservern, Tendenz steigend.
Mehr als 200.000 neue Domains werden jeden Tag registriert – davon werden mehr als 70% als gefährlich eingestuft und werden somit auf unserer Plattform nicht aufgenommen.

Blue Shield Security GmbH | Kornstraße 7A | 4060 Leonding | AUSTRIA | **www.blue-shield.at**

FALLSTUDIE FÜR DIE VERSICHERUNGSBRANCHE

AKTUELLE HERAUSFORDERUNGEN

- Oft keine einheitliche Endgeräte-Struktur - **blinde Flecken in der Infrastruktur** aufgrund nicht oder nur unzureichend verwalteter Geräte führen zu Sicherheitsproblemen
- Auch nach Sensibilisierungsmaßnahmen **klicken Mitarbeiter immer noch auf bösartige Links** oder Phishing-Mails
- Hoher Anteil an mobilen Außendienstmitarbeitern und Agenturen – diese sind aufgrund vieler Schnittstellen zu externen Partnern und in fremden WLANs immer häufiger Bedrohungen ausgesetzt und damit ein Einfallstor für Sicherheitsprobleme in das interne Firmennetzwerk
- **„Bring your own device"-Problematik** macht oft ein dynamisches Sicherheitskonzept nötig
- Bestehende Lösungen hinken neuen Bedrohungen immer einen Schritt hinterher.
  Dies führt zur **Überlastung von IT-Security Mitarbeitern**

ZIELSETZUNG

- **Einfach und nahtlos zu implementieren**
- Keine oder nur wenige interne Ressourcen während der Einrichtung und des Betriebs erforderlich
- Deckt **alle Arten von Endgeräten** (stationär, mobil, Smartphones, Tablets) ab
- Erlangung datengestützter Erkenntnisse und Kennzahlen zur Wahrnehmung der Bedrohungen

ERGEBNISSE

- Zentrale **Implementierung in unter 30 Minuten**
- Erfolgreiche **Phishing-Kampagnen um über 90% reduziert**
- Der Whitelist/Allowlist-Ansatz von BlueShield Umbrella **schafft einen Zeitpuffer für die IT- und Sicherheitsabteilung**, auf neue Bedrohungen zu reagieren
- Neue Kennzahlen zur Bewertung von Effektivität der Maßnahmen für das Management
- Jede einzelne **blockierte Domäne zum betroffenen Gerät nachverfolgbar**

DERZEIT BLOCKIEREN WIR IM DURCHSCHNITT EINE ALS GEFÄHRLICH EINGESTUFTE ANFRAGE PRO BENUTZER/ PRO TAG IN DER VERSICHERUNGSBRANCHE.

FAKTEN ZU BLUE SHIELD

- Gegründet 2015 im Herzen Europas
- Über 30 Mitarbeiter im Bereich Forschung & Entwicklung
- **Einzigartige KI-basierte Whitelist/Allowlist-DNS-Filterung**
- Mehr als 700 Kunden (Stand: Juni 2020) vertrauen BlueShield.
  100%ige Verlängerungsquote.

REFERENZKUNDEN:

wüstenrot · NV Die Niederösterreichische Versicherung · VAV VERSICHERUNGEN · VIG VIENNA INSURANCE GROUP

Blue Shield Security GmbH | Kornstraße 7A | 4060 Leonding | AUSTRIA | **www.blue-shield.at**

BlueShield