Central Threat Intelligence mit Blue Shield Umbrella

IT Sicherheit der Zukunft

Central Threat Intelligence mit Blue Shield Umbrella

IT Sicherheit der Zukunft

Aktuelle Sicherheitslage

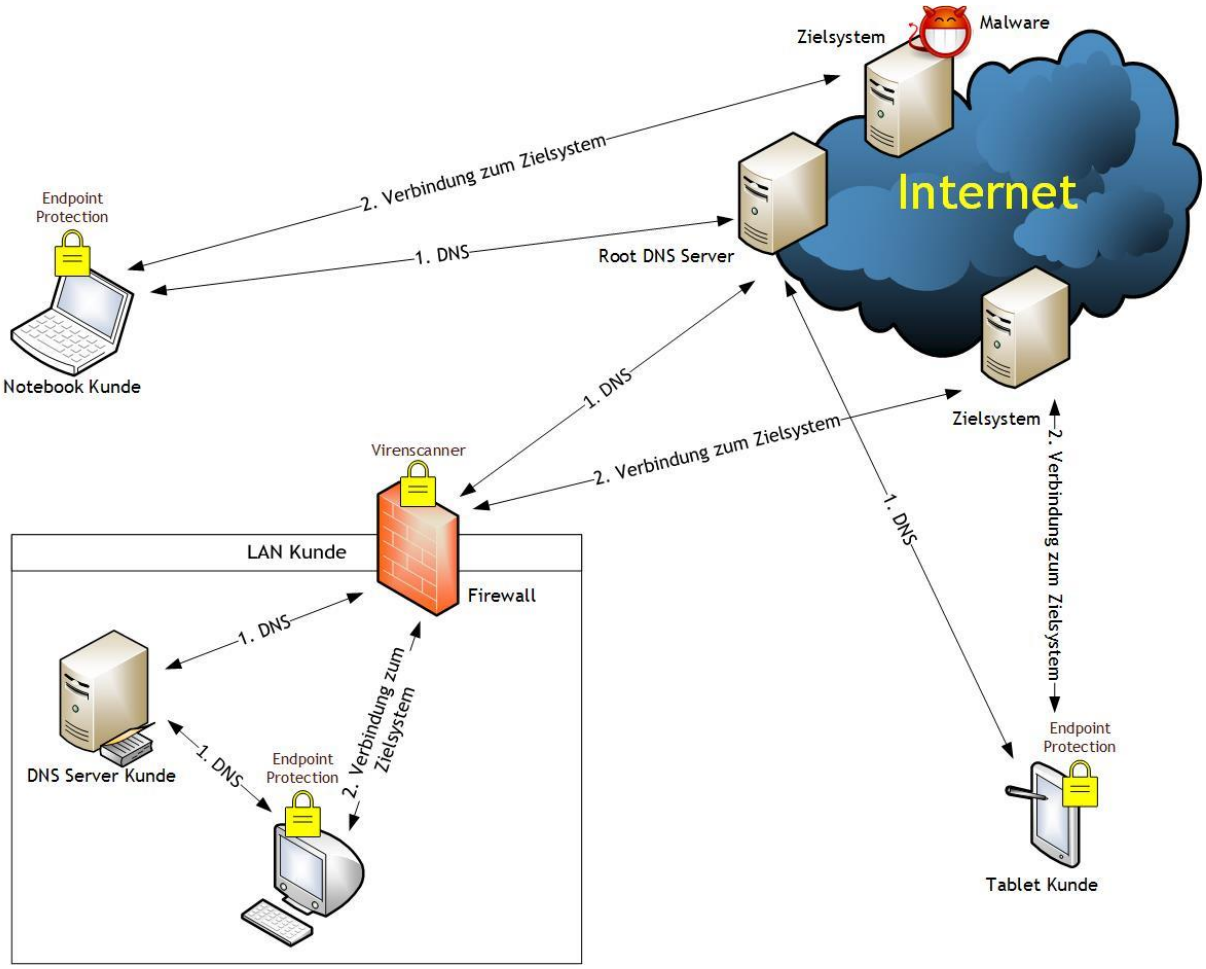
Unternehmen jeder Größe und Branche sehen sich heutzutage ständig den Gefahren aus dem Internet ausgesetzt. Egal ob dies durch ungezielte Breitbandangriffe (z.B. Ransomware) oder zielgerichtete Attacken (z.B. CEO Fraud) passiert, Kriminelle schlagen im Internet meist unerkannt und blitzschnell zu. Die Schäden können mittlerweile gigantisch und existenzbedrohend sein. Ob im Radio, TV oder in der Presse - inzwischen werden täglich Fälle vermeldet. Zudem werden CyberCrime Attacken zunehmend kommerzialisiert. Ein Geschäftsmodell der Zukunft liegt in Malware-as-a-Service, bei dem Laien Steuerserver und Schadsoftware mieten können.

Wie schützen sich Unternehmen heute

Die IT-Abteilungen der Unternehmen sehen sich, neben Projekten und dem Tagesgeschäft, zunehmend mehr den Gefahren aus dem Cyberraum ausgesetzt. Ein Schutz für das Unternehmen wird meist aus mehreren Komponenten bereitgestellt. Dazu zählen Firewalls, Sandboxsysteme, Intrusion Prevention Systeme, Endpoint Protection und vieles mehr. Alles ist darauf ausgerichtet, die Daten und Infrastrukturen vor einer Kompromittierung zu schützen. Optimalerweise wird die Schadsoftware bereits vor oder am Netzübergang zum LAN abgefangen, wie z.B. mit Firewalls, AntiSPAM, Proxys und Intrusion Prevention Systemen. Sollte ein Schädling durchkommen, soll die Endpoint Protection eingreifen und für Schutz sorgen.

Alle diese Systeme sind stetig aktuell zu halten und zu überwachen. Der administrative Aufwand dafür ist erheblich, wenn man ein gut funktionierendes Sicherheitssystem erwartet. Trotzdem gelingt es den Internetkriminellen immer wieder mit neuester Schadsoftware die IT-Sicherheitssysteme zu überlisten und erfolgreich anzugreifen.

Internetkommunikation
Standard heute



Ist die Schadsoftware erst einmal ins LAN gelangt,
sind wirksame Gegenmaßnahmen häufig zu spät.

Wie funktionieren aktuelle Virenscanner

Virenscanner arbeiten mit verschiedenen Methoden, um Schadsoftware zu erkennen. Die wichtigsten und meist verwendeten sollen nachfolgend kurz erläutert werden:

Signaturen
Um bekannte Viren zu erkennen und zu isolieren, verteilen Antivirenhersteller sogenannte Signaturen an ihre Clients. Diese Methode schützt allerdings nur unter der Voraussetzung, dass die Schadsoftware bereits bekannt und identifiziert ist. Des Weiteren nehmen die Erstellung sowie die Verteilung einer Signatur viel Zeit in Anspruch.

Heuristik
So wird die Suche nach allgemeinen Merkmalen und Auffälligkeiten bezeichnet, um eine noch unbekannte Schadsoftware zu erkennen. Dafür ist eine besondere Intelligenz der Antivirensoftware nötig, welche sehr aufwendig zu programmieren und aktuell zu halten ist, da „normale“ Programme ja nicht beeinträchtigt werden sollen.

Sandboxing
In einer virtuellen Umgebung soll eine vermeintliche Schadsoftware zu Aktivitäten animiert werden. Sobald das Schadprogramm loslegt, kann es erkannt und isoliert werden, ohne dass es in die Produktivumgebung gerät.

Verhaltensanalyse
Ähnlich wie bei der Heuristik und dem Sandboxing wird auch hier das Verhalten analysiert, jedoch unter Einsatz von Algorithmen (z.B. genetische oder trainierbare) sowie von Statistiken und neuronalen Netzwerken. Dies ist eine sehr wirksame Methode, welche aber in der Regel nur in Echtzeit auf dem Produktivsystem ausgeführt wird.

Das Problem liegt in der Natur der Sache

Die meisten IT-Sicherheitslösungen arbeiten mit den oben beschriebenen Methoden, welche bei weitem nicht mehr dem Stand der Technik entsprechen. Die Hersteller von Schadsoftware testen ihre Programme mit den aktuellsten Virenscannern, um die Erkennungsrate festzustellen. Auch Sandboxing wird von den meisten Schadprogrammen erkannt und diese reagieren nicht mehr, bis sie wieder aus der Sandbox entlassen werden. Die Arten der Angriffe werden immer komplexer, sind einfach und automatisch zu verändern, sodass eine Mustererkennung nicht greift. Auf neue Bedrohungen kann somit nur sehr zeitversetzt reagiert werden. Wenn die Schadsoftware erstmal ins LAN gelangt ist, sind wirksame Gegenmaßnahmen häufig schon zu spät. Moderne Malware ist auch in der Lage, sich jederzeit up to date zu halten, indem sie aktualisierte Komponenten nachlädt. Nebenbei stellen moderne Endpoint Protection Systeme auch hohe Anforderungen an die Leistungsfähigkeit eines Arbeitsplatzsystems. Kurzum: Es fehlt an echten Innovationen im Bereich der IT-Sicherheit.

Die Lösung mit Blue Shield

Vollschutz gegen Schadsoftware Umbrella

Harmlos aussehende Emails, kompromittierte Webseiten und sogenannte Drive-by Attacken sind die gängigsten Wege um Schadsoftware zum Angriffsziel zu transportieren. Dort angelangt, sind annähernd 100% aller Schadsoftware in der Lage über das Internet einen Code zu laden, welcher es ermöglicht den Angriff im LAN zu starten und auszuführen.

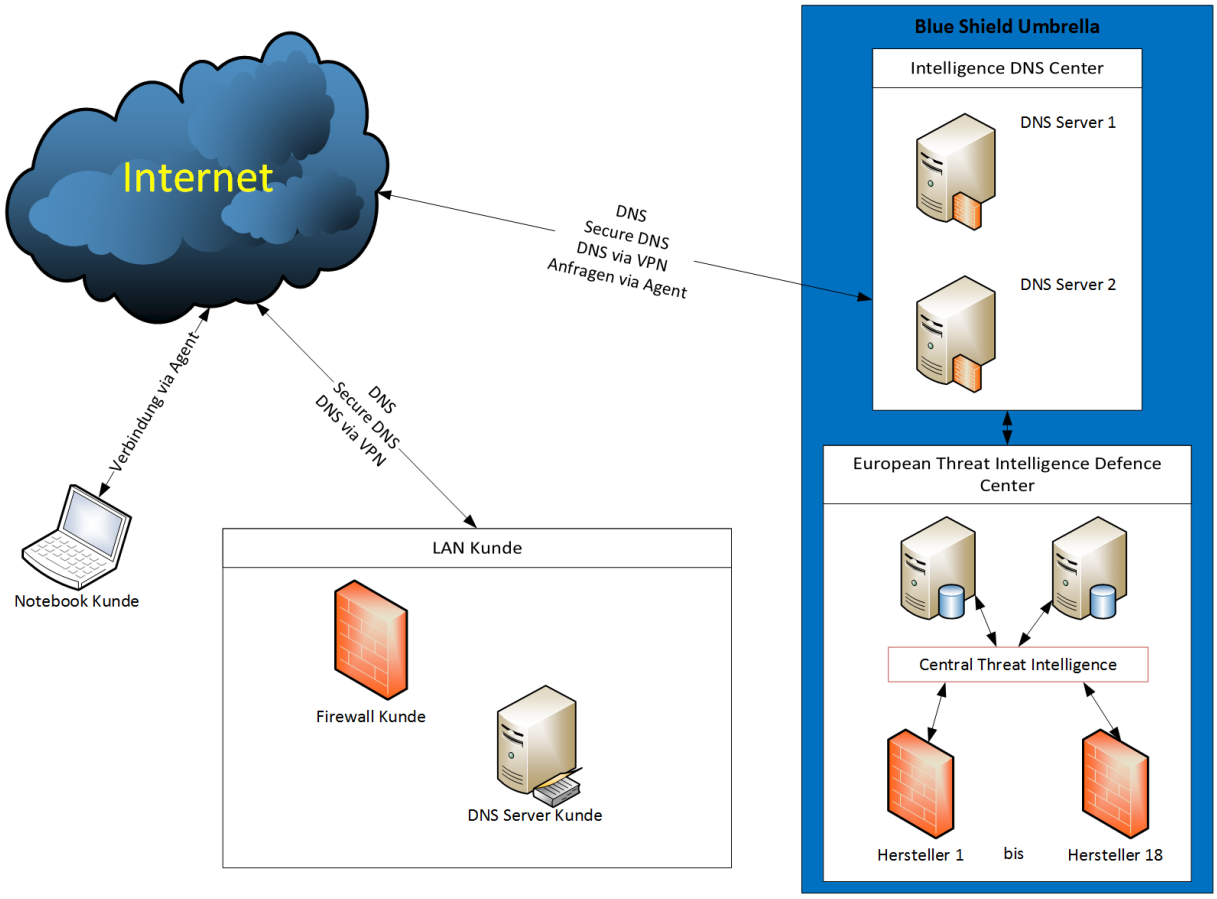
Dies geschieht fast ausschließlich mit Hilfe von DNS (Namensauflösung). Der Link in einer E-Mail führt über einen Namen zu einem kompromittierten Server und lädt dort, ohne dass der Benutzer es merkt, einen Schadcode herunter und führt diesen sofort oder zeitgesteuert aus. Das Problem ist, dass über die Namensauflösung der Link nicht sofort als kompromittiert erkannt wird und so der Angriff erstmal erfolgt. Je nachdem wie gut die vorhandenen Sicherheitssysteme sind, kann die Attacke meist nicht verhindert, aber zumindest entdeckt und ggf. unterbunden werden.

Um nun den Angriff an sich zu verhindern, muss der Name des kompromittierten Systems bekannt sein und gesperrt werden. Das bietet den vollständigen Schutz, dass Schadsoftware nicht auf die IT-Systeme gelangt. Die Namensserver im LAN, ein DNS Proxy, eine Firewall oder ein Router lösen ihre Namensanfragen lokal auf und leiten diese im Bedarfsfall an die sogenannten Root-DNS-Server weiter. Dort erhalten sie die Antworten zur Namensauflösung zurück und versorgen damit ihre Clients.

Anstelle von Root-DNS-Servern werden nun die Intelligence DNS Center für die Namensauflösung angefragt. Diese kommunizieren mit dem European Threat Intelligence Defence Center und erhalten von dort in Echtzeit eine Bewertung der angefragten Namen. Ist ein Name gesperrt, wird der anfragende Server darüber informiert und die Clients erhalten eine Meldung über die Sperrung. Mit dieser innovativen Technik wird ein Angriff schon unterbunden bevor er erfolgt und das Nachladen von Schadcodes verhindert. Auch die Funktion vorhandener Botnetze, Trojaner oder ähnlichem wird ab dem Einsatz dieser modernen Technologie abgeschaltet. Eine Kommunikation mit den Steuerungsservern ist nicht mehr möglich und die Schadsoftware ist wirkungslos. Dadurch wird diese im LAN auch transparent, da zwar die Kommunikation mit den Steuerservern nicht mehr funktioniert, aber trotzdem versucht wird.

Das European Threat Intelligence Defence Center überprüft mit zahlreichen Techniken die angefragten Server im Internet auf Kompromittierung und speichert die Ergebnisse in einer Datenbank. Hier werden unter anderem auch mathematische Berechnungen einbezogen. Die Gefahren werden somit nicht nur erkannt, sondern ausgesperrt.

DNS Kommunikation mit Blue Shield Umbrella



- Zentrale Cloud basierte Threat Intelligence
- Schnell und flexibel dank DNS Verwendung
- Schützt sämtliche IP basierten Devices
- Windows/MacOS/IOS/Android/Linux/ Internet of Things/Industrie 4.0
- Simples Deployment mittels Software-as-a-Service

Implementierung ganz einfach

Bei den meisten IT-Sicherheitslösungen muss ein großer Aufwand für die Implementierung im LAN sowie für den Betrieb und die Schulung der Mitarbeiter der zuständigen IT-Abteilung betrieben werden. Dies entfällt mit Blue Shield Umbrella. Es ist lediglich die Umstellung auf die Intelligence DNS Center notwendig. Die vorhandene Firewall muss noch konfiguriert werden, damit sie Anfragen zur Namensauflösung nur von den autorisierten DNS Servern im LAN erlaubt. Bei mobilen Arbeitsplätzen muss ein Agent ausgerollt werden, der sicherstellt, dass außerhalb des sicheren LANs immer der richtige DNS-Server gefragt wird und nicht verändert werden kann. Damit ist die Implementierung abgeschlossen und der Schutz ist aktiv. Einfacher geht es nicht.

Blue Shield Umbrella verbraucht keinerlei Ressourcen (von z.B. Festplatte, CPU, Arbeitsspeicher) in Ihrer Systemumgebung, da keine Softwarekomponenten installiert werden müssen. Eine Installation betrifft lediglich jene Geräte, welche auch außerhalb des LANs genutzt werden.

Reporting und Zustandsbericht

Während des aktiven Schutzes erhalten Sie Reports und Zustandsberichte, die Ihnen die abgewehrten Gefahren aufzeigen. Diese können Sie ganz einfach in Ihrem persönlichen Kundenportal einsehen. Dadurch sind Sie unter anderem in der Lage, vorhandene Schädlinge im Netz - welche durch Blue Shield Umbrella an der Kommunikation gehindert werden, jedoch noch vorhanden sind - endgültig zu deinstallieren und zu entfernen. Weiterhin können Sie Rückschlüsse über das Verhalten Ihrer Clients in Bezug auf die IT Sicherheit und deren Nutzung ziehen.

Das technische Konzept

Auf Seite des Kunden wird optional für Windows Notebooks und Tablets ein Agent ausgerollt, der sicherstellt, dass außerhalb des sicheren LANs immer die DNS Server des Intelligence DNS Centers verwendet werden und nur diese den DNS Verkehr erhalten und beantworten. Im LAN des Kunden werden auf den DNS Servern die Root-DNS Server deaktiviert und die DNS Server des Intelligence DNS Center eingetragen. Auf LAN Seite der Firewall wird eine Regel konfiguriert, die ausgehende DNS Abfragen nur durch die autorisierten DNS Server im LAN erlaubt. Die Firewall erhält als DNS Server Eintrag ebenso die DNS Server des Intelligence DNS Center. Die Kommunikation zwischen dem Kunden und dem Intelligence DNS Center erfolgt wahlweise via Agent, DNS, Secure DNS oder mittels eines VPN Tunnels. Bei der Kommunikation verlassen keinerlei sensible oder personenbezogene Daten das LAN.

Das Intelligence DNS Center gibt es mehrfach und beantwortet die DNS Anfragen der Kunden. Weiterhin stellt es die Kommunikation mit dem European Threat Intelligence Defence Center sicher. Das Intelligence DNS Center ist redundant ausgelegt.

Das European Threat Intelligence Defence Center ist das Herzstück des Systems, dies ist ebenso redundant ausgelegt und analysiert rund um die Uhr in Echtzeit Mailserver und Webseiten im Internet. In der Central Threat Intelligence werden durch besondere mathematische Algorithmen und voraus-

schauende (predictive) Analysen, Gefahren errechnet und die damit im Zusammenhang stehenden Server blockiert. Zusätzlich werden IT-Sicherheitsmechanismen aus einem Pool der 14 größten Security Hersteller weltweit abgefragt und in die Bewertung miteinbezogen. Dies stellt aktuell das vermutlich umfangreichste und sicherste Verfahren zur Bewertung von Webseiten und Mailservern im Internet dar.

Blue Shield Umbrella besteht damit aus den beiden Komponenten Intelligence DNS Center und dem European Threat Intelligence Defence Center.

Die Zielgruppen von Blue Shield Umbrella

Blue Shield Umbrella eignet sich für jede Unternehmensgröße sowie für jeden erdenklichen Geschäftszweig. Egal ob Handel, Produktion, Versorger oder andere Branchen – von dem umfangreichen Schutz dieser neuartigen Enterprise Technologie profitieren alle. Dank einfachster Implementierung ist es möglich, schnell und sauber einen Schutz in hoher Geschwindigkeit bereitzustellen.

Besonders interessant ist Blue Shield Umbrella für Carrier. Durch einen zentralen Rollout und die zentrale Steuerung der Gateways ihrer Kunden kann deren Schutz drastisch erhöht werden. Außerdem lässt sich hier ein zusätzlicher Nutzen abbilden und darstellen. Der Schutz kann als Zusatzgeschäft mit einer Internetleitung verkauft werden.

Auch Privatpersonen und Haushalte können sich mit der Blue Shield Umbrella Technologie einfach und bequem schützen. Durch das simple Umstellen der Namensauflösung am Gateway ist der Schutz zu Hause sofort gewährleistet und auch für Laien machbar.

Die Vorteile von Blue Shield Umbrella im Überblick

- ✓ Innovativste und modernste Erkennung von Schadsoftware in Echtzeit
- ✓ Kombination von bekannten Erkennungsmethoden und vorrausschauenden Berechnungen durch mathematische Algorithmen bietet den höchsten Schutz gegen Malware
- ✓ Die Prüfung findet außerhalb Ihres LANs statt, somit kommt potentielle Schadsoftware gar nicht mehr in Ihr Netz
- ✓ Einfachste Implementierung und Rollout
- ✓ Keine Installation von Software im LAN notwendig
- ✓ Kein Verbrauch von teuren Ressourcen wie Rechenleistung, Arbeitsspeicher oder Festplatte
- ✓ Keine Updatemechanismen notwendig und damit auch keine Überprüfung der Updatefunktion
- ✓ Kein administrativer Aufwand notwendig
- ✓ Abgewehrte Gefahren und messbare Wirksamkeit im Portal einsehbar
- ✓ Unabhängig von der eingesetzten IT-Landschaft und den Betriebssystemen im LAN
- ✓ Schutz auch von alten Systemen, wie z.B. Windows 95 oder XP gegeben
- ✓ Schutz von proprietären Systemen und Industrial IT Komponenten
- ✓ Keinerlei Übertragung von personenbezogenen Daten

Glossar

Intelligence DNS Center

Das Intelligence DNS Center stellt die Server zur Namensauflösung bereit. Der Endkunde muss sämtliche DNS Anfragen an diese Server weiterleiten, um Blue Shield Umbrella zu nutzen. Sie stellen die Kommunikation zum European Intelligence Threat Defence Center bereit.

Central Threat Intelligence

Dort werden permanent Server im Internet mit mathematischen Algorithmen geprüft und die Wahrscheinlichkeit einer Bedrohung errechnet. Weiterhin laufen hier auch zentral die Informationen der ausgewählten, größten IT Security Hersteller ein und werden verarbeitet. Diese Erkenntnisse werden in den Datenbanken des European Threat Intelligence Defence Center eingespeist.

European Threat Intelligence Defence Center

Das European Threat Intelligence Defence Center ist mit der Central Threat Intelligence das Herzstück der Blue Shield Umbrella Lösung. Hier stehen die Datenbankserver, welche von der Central Threat Intelligence mit den Ergebnissen aus den mathematischen Wahrscheinlichkeitsberechnungen und Informationen der ausgewählten IT Security Hersteller gespeist werden. Von hier werden die Informationen an die Intelligence DNS Center ausgeliefert. Das European Threat Intelligence Defence Center ist redundant in mehreren Rechenzentren aktiv.

Blue Shield Umbrella

Blue Shield Umbrella ist eine der wirkungsvollsten, modernsten und innovativsten Sicherheitslösungen gegen Schadsoftware. Die Lösung besteht aus den Cloud-Komponenten Intelligence DNS Center, European Threat Intelligence Defence Center und Central Threat Intelligence. Der Endkunde muss nur seinen DNS Verkehr an das Intelligence DNS Center weiterleiten, um den Blue Shield Umbrella Schutz zu erhalten.

Weitere Informationen erhalten Sie über:

Blue Shield Security GmbH
+43 732 211 922
office@blue-shield.at
www.blue-shield.at

Kornstraße 7a
4060 Leonding
Österreich

Raum für Ihre Notizen:

ordino

in reihe bringen

Beratung in Strategie & Logistik, Schwerpunkt Prozess orientiert
IT Umsetzungen in Sicherheit , Virtualisierung und Netzwerkmanagement

Ordino e.U.
+43 664 161 4975
office@ordino.at
www.ordino.at

Reichsstraße 126
6800 Feldkirch
Österreich