CryptoApp

Funktionsbeschreibung

Version 2.50

CryptoMagic
Werner-von-Siemens Str. 6
86159 Augsburg

Tel: 0821 / 217 009 – 0
Fax.: 0821 / 217 009 – 99

E-Mail: info@cryptomagic.eu

Stand: 08.11.2017

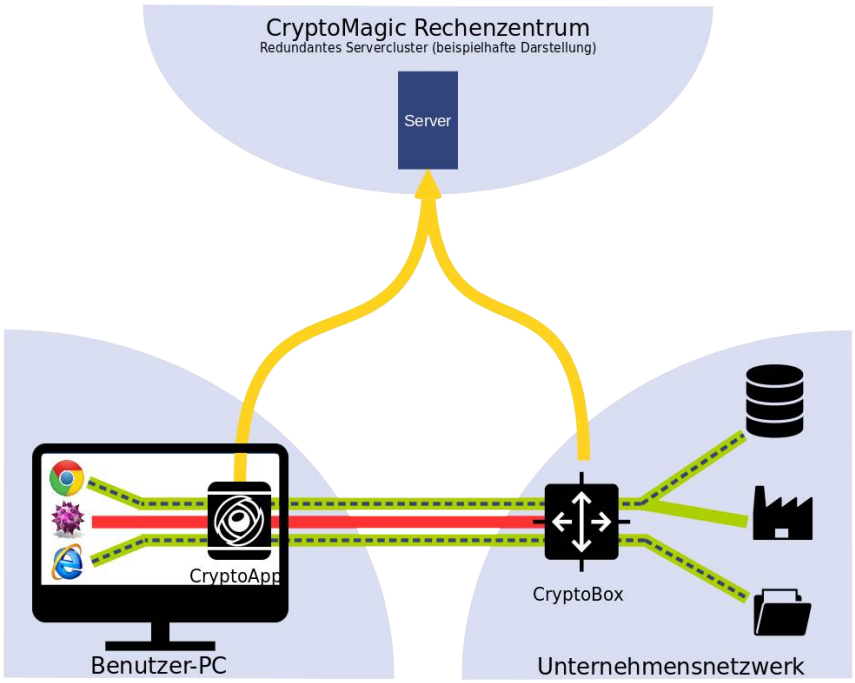
1. Inhalt

1. CryptoApp Aufbau

CryptoApp besteht aus drei Elementen, welche im Zusammenspiel eine neuartige und einfache Datenübertragung über potentiell unsichere Netze ermöglicht, die im Vergleich zu etablierten Lösungen neue Sicherheitsmaßnahmen ermöglicht.

Als Datenübertragung ist in diesem Zusammenhang der Zugriff von Anwendungen eines Client-PCs auf Dienste eines entfernten Netzwerkes zu sehen; ähnlich wie bei einem VPN werden TCP/IP basierte Datenverbindungen verschlüsselt und vertraulich übertragen. Dies wird allerdings nicht auf Paketebene mittels virtueller Netzwerkkarten ermöglicht, sondern durch Abgreifen der Verbindungen in der Anwendung, bevor diese Verbindungen an das Betriebssystem zur Übermittlung gelangen.

Für weitere Informationen hierzu siehe unser Dokument *CryptoApp – die Technologie,* sowie in diesem Dokument 2. CryptoApp Verfahren.



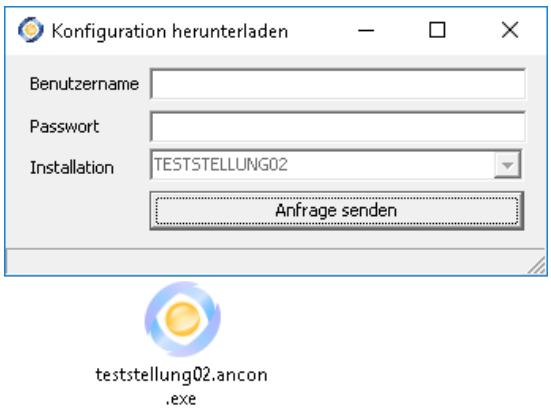
1.1 CrytpoApp Client

Ein Element von CryptoApp stellt die portable Clientsoftware dar, die bereits für Microsoft Windows vorliegt, und sich für Linux sowie macOS in Entwicklung befindet. Diese kann entweder auf mehreren Systemen über einen mobilen Datenträger (z.B. USB-Stick), oder dauerhaft an einen bestimmten PC gebunden genutzt werden.

Portabel bedeutet in diesem Zusammenhang:

- Keine Installation – lediglich direkte Ausführung
- Keine Administrationsberechtigungen notwendig
- Keine Abhängigkeiten in Form von Bibliotheken, Frameworks oder Ähnlichem
- Keine persistenten Änderungen

1.1.1 Deployment und Konfiguration

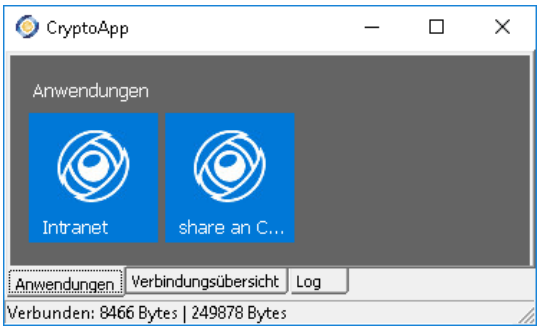


Die Clientsoftware wird entweder vorkonfiguriert ausgeliefert, in dem die Konfiguration heruntergeladen und mit der Clientsoftware zusammen ausgeliefert wird, oder der Client bezieht die Konfiguration bei der ersten Ausführung.

Hierzu existieren Installationskennungen, mit der die jeweilige CryptoApp Installation spezifiziert wird. Diese kann bei der Auslieferung der Clientsoftware über den Dateinamen vorgeblendet werden, so dass lediglich Authentifizierungsinformationen vom Anwender anzugeben sind. Diese können gegenüber einen Verzeichnissdienst, wie beispielweise Active Directory, LDAP, REST-APIs, Webseitenlogins oder ähnlichem geprüft werden. Mehr Details hierzu finden Sie im Administrationshandbuch zu CryptoApp.

Hierzu bezieht der Client als Erstes vom CryptoMagic RZ die Informationen, um mit der entsprechenden CryptoApp Installation vertrauenswürdig und verschlüsselt kommunizieren zu können. Es wird hierzu vom Client lediglich die Installationskennung übermittelt, um diese Informationen abzufragen. Im zweiten Schritt wird eine Verbindung zur CryptoBox des Kunden aufgebaut, und mittels der Authentifizierungsinformationen die Verbindungsparameter (Host, IP, Clientzertifkat) abgerufen. Alle weiteren Konfigurationsoptionen werden zur Laufzeit, beim Verbinden des Clients, übermittelt und nicht vorgehalten.

1.1.2 Anwendermenü



Die Clientsoftware öffnet nach den Starten unverzüglich eine Übersicht von Anwendungen, die dem Anwender zur Verfügung stehen.

Die Übersicht, die hier erscheint, wird vom Konfigurationsserver festgelegt und dient lediglich der Vereinfachung: Der Benutzer kann die Anwendungen auch selbst öffnen und die Übertragung über CryptoApp kommt genauso zum Tragen.

1.1.3 Hardwarebindung

Die Clientsoftware übermittelt beim Verbinden eine Hardwarekennung, über welche eine Bindung an den vorliegenden Datenträger oder das System durchgeführt wird. Im Falle eines mobilen Datenträgers, beispielsweise einen USB-Stick, wird die Nutzung auf wechselnden PCs wird in Verbindung mit diesem Datenträger zugelassen. Beim Starten von Festplatte wird hingegen eine Bindung an die Festplatte des aktuellen PCs vorgenommen.

1.1.4 Datenübertragung

Die Clientsoftware stellt eine verschlüsselte und gesicherte Ende-zu-Ende Verbindung zur gegenüberliegenden CryptoBox her, um Verbindungen ins entfernte Netzwerk herzustellen. Der Client wird über ein Clientzertifikat identifiziert, welches die alleinige persistente lokale Konfiguration darstellt.

Um Verbindungsproblemen vorzubeugen, kann die Verbindung über ein Rendezvous im Rechenzentrum der CryptoMagic hergestellt werden, ohne dass hierbei die Ende-zu-Ende Verbindung aufgebrochen wird: Insbesondere um NAT- und Firewall Problematiken zu vermeiden, ist dies hilffreich. Das Rendezvous ist insbesondere dann hilfreich, wenn SSL-Verbindungen nur über HTTP(S)-Proxies aus gesicherten Firmennetzwerken übertragen werden können, sowie bei fehlenden Portweiterleitungen oder Filterregeln.

Der Client kommuniziert ausschließlich per TLS mittels folgender Parameter:

- Verschlüsselungsprotokoll TLS 1.2
- Schlüsselaustausch PFS / DH
- Verschlüsselung AES 256
- Übertragungssicherung GCM
- Authentifizierung X.509
  RSA 4096 oder RSA 2048(alt)

Hierfür wird pro Kunde eine eigene CA verwaltet, und der Client vertraut zur Datenübertragung nur von dieser eigenen CA signierten Zertifikaten. Der Client vertraut zudem zum Abruf der Installationskennungen (Siehe 1.1.1 Deployment und Konfiguration) einer CA der CryptoMagic, die unveränderbar im Client hinterlegt ist. Zur Überprüfung der CA und deren ausgestellten Zertifikate ist eine korrekte Uhrzeit auf allen beteiligten Systemen notwendig.

Die Clientsoftware verbindet sich, wenn diese unkonfiguriert ausgeliefert wurde, neben dem Rendezvous auch zur Erstkonfiguration ins Rechenzentrum. Für beide Funktionen ist es erforderlich, dass die folgende Verbindung ermöglicht wird:

- Protokoll TCP
  TLS 1.2 [over HTTPS]
- Host ca.cryptoapp.cryptomagic.eu
  cryptoapp.cryptomagic.eu
  wechselnde, mehrere IPs!
- Port 443

1.1.5 Aktualisierungen und Updates

Der Client kann selbstständig Updates anwenden, die von der CryptoBox des Kunden ausgeliefert werden. Insbesondere um die SSL-Bibliotkek OpenSSL aktuell zu halten, ist ein zeitnahes und automatisiertes Update empfehlenswert.

Auch das Clientzertifikat sowie die Verbindungsoptionen des Clients können von der CryptoBox aktualisiert werden, wenn lokale Schreibberchtigungen vorliegen.

1.2. CryptoBox

Eine weiteres Element von CryptoApp stellt die CryptoBox dar, welche in den Zielnetzwerken aufgestellt wird. Diese wird von den Clients angesprochen, um eine verschlüsselte und vertrauenswürdige Verbindung aufzubauen und hierüber Verbindungen ins Netzwerk herstellen zu können.

1.2.1 Formen

Die CryptoBox ist als Hardware Appliance sowie als Softwarelösung beziehbar, die unter Windows oder Linux laufen kann; letzeres auch auf embedded Devices. Beide Softwareversionen sind auch virtualisiert einsetzbar.

Im Falle einer Hardware Appliance wird diese vom Distributionspartner vorkonfiguriert ausgeliefert. Als Softwarelösung kann die Konfiguration in der Oberfläche heruntergeladen werden, und im Rahmen der Installation abgefragt.

1.2.2 Deployment

Das Deployment einer CryptoBox besteht darin, diese am Zielstandort ans Netzwerk anzuschließen bzw. zusammen mit der heruntergeladenen Konfiguration auszuführen sowie zu überprüfen, dass sich diese erfolgreich zum Konfigurationsserver verbinden kann.

1.2.3 Netzwerk- oder Internetverbindung

Die CryptoBox verbindet sich dauerhaft ins Rechenzentrum der CryptoMagic, um dort auf den Konfigurationsserver zuzugreifen, die aktuelle Uhrzeit zu beziehen sowie das Rendezvous mit Clients zu ermöglichen (Siehe 1.1.4 Datenübertragung). Die Anforderungen an Filterregeln und Netzwerkverbindungen hierzu sind die gleichen, wie dies für den Client der Fall ist (Siehe 1.1.4 Datenübertragung).

Stellt der Client die Verbindung zur CryptoBox direkt, d.h. ohne Rendezvous im Rechenzenturm, her, so ist es erforderlich dass der zur Verbindung konfigurierte Host per DNS auflösbar ist, und dass die Verbindung ausgehend vom Client mittels des konfigurierten Ports zur CryptoBox aufbaubar ist: Insbesondere ist dafür zu sorgen, dass auf Routern und Firewalls entsprechende Routing- und Filterregeln und/oder Portweiterleitungen angelegt worden sind.

1.2.4 Virtualisierung

Die CryptoBox kann in allen etablierten virtualisierten Umgebungen betrieben werden, Sie müssen lediglich zunächst Linux oder Windows installieren um im Anschluss die CryptoBox in diesem Betriebssystem installieren zu können.

Als Virtualisierungslösung stehen Ihnen alle gängigen Lösungen zur Verfügung, die ein Windows- oder Linux-System unterstützen. Dies sind beispielsweise die Folgenden:

Docker / ESXi / HyperV / KVM / LXC / VirtualBox / VMWare / XEN

Weitergehende Informationen zum jeweiligen Betriebssystem finden Sie unter den nachfol-

genden Punkten 1.2.5 Windows und 1.2.6 Linux.

1.2.5 Windows

Für Microsoft Windows erhalten Sie ein etwa 8 MB großes MSI-Installationspaket, welches Sie per Doppelklick installieren können.

Die Software ist unter allen x86/x64 Windows-Versionen ab Windows XP / Server 2003 einsetzbar, und stellt keine Anforderungen an Bibliotheken, Frameworks oder Ähnlichem.

1.2.6 Linux

Für Linux bieten wir Ihnen jeweils eine etwa 10 MB große direkt ausführbare Datei an, die für allen gängigen Linuxdistributionen auf den Platformen x86, x64 sowie ARM verfügbar ist.

Dies umfasst somit alle aktuellen Distributionen, natürlich auch die Folgenden:

Arch Linux / Debian Linux / RedHat / SuSE / Ubuntu

1.2.7 ARM (Embedded)

Für embedded Systeme unter Linux bieten wir für die armhf sowie arm64 Plattform eine jeweils eigene Version von wenigen MB an. Mittels dieser können Sie nicht nur auf Geräten wie auf einem Odroid oder Raspberry eine CryptoBox laufen lassen, sondern auch auf vielen anderen ARM-Basierten Geräten wie Network Attached Storages, Netzwerkroutern oder Ähnlichem.

Desweiteren gelten die gleichen Punkte wie unter 1.2.6 Linux beschrieben.

1.2.8 Aktualisierungen und Updates

Die CryptoBox kann vom Konfigurationssystem Updates erhalten, für sich sowie für angeschlossene CryptoBoxen. Insbesondere um die SSL-Bibliotkek OpenSSL aktuell zu halten, ist ein zeitnahes und automatisiertes Update empfehlenswert.

Auch die Zertifikat sowie die Verbindungsoptionen können aktualisiert werden, wenn lokale Schreibberchtigungen vorliegen.

1.3. Konfigurationsserver

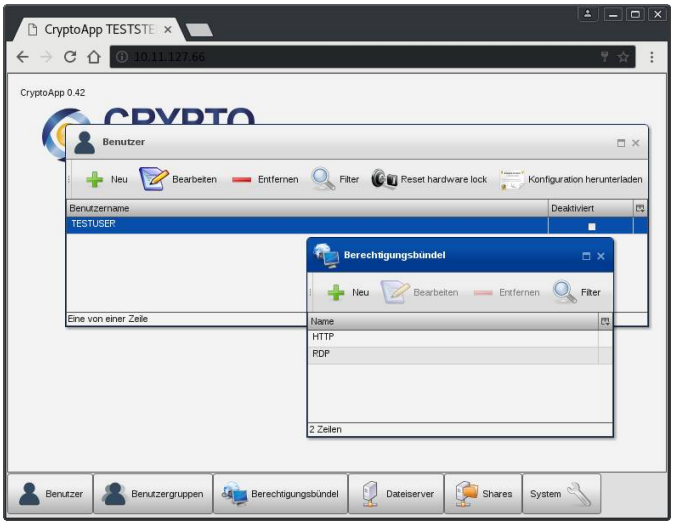
Das zentrale Element von CryptoApp ist der Konfigurationsserver, in dem alle Einstellungen zentral gespeichert werden.

1.3.1 Aufbau

Das Konfigurationssystem basiert auf der Eigenentwicklung ADBGUI, das unter Linux läuft.

Dieses basiert auf Qooxdoo(http://www.qooxdoo.org/), MariaDB(https://mariadb.org/) sowie dem POE Framework(http://poe.perl.org/).

1.3.2 Bedienoberfläche



Die Benutzeroberfläche für Endbenutzer stellt eine Oberfläche dar, die durch das Qooxdoo-Framework hergestellt wird. Hierüber sind alle Konfigurationseinstellungen durchführbar, die von der CryptoBox als auch dem Client zur Laufzeit abgefragt werden.

Weitere Informationen zu den Konfigurationsmöglichkeiten, finden Sie im Administrationshandbuch.

1.3.3 Schnittstellen

Das ADBGUI-Framework bietet als Maschine-zu-Maschine Schnittstelle eine REST API (https://de.wikipedia.org/wiki/Representational_State_Transfer) an, mit der grundlegende als auch höherliegende Funktionen angesteuert werde können. Die Abfrage- als auch Übergabe von Informationen wird hierbei in Form von JSON Objekten (https://de.wikipedia.org/wiki/JavaScript_Object_Notation) durchgeführt.

Es ist hierüber beispielsweise möglich, automatisiert Benutzer, Berechtigungsbündel sowie deren Zuordnung vorzunehmen oder auszulesen.

1.3.4 Zeritifkatsverwaltung

Die zentrale Aufgabe des Konfigurationsservers ist die Verwaltung einer installationsspezifischen X.509 Certificate Authority (CA). Für jeden Client und CryptoBox werden entsprechende Zertifikate standardkonform ausgestellt und an diese verteilt. Hierfür haben wir eine spezielle Bibliothek entwickelt, die es uns ermöglicht Zertifikate automatisiert und vollumfänglich standardkonform zu erzeugen und die CA zu warten.

Alle Funktionalität wird an die eindeutig vergebene ID des jeweiligen Zertifikates gebunden, alle weiteren Daten des Zertifikates werden lediglich zur Bestimmung seiner allgemeinen Gültigkeit herangezogen.

2. CryptoApp Verfahren

CryptoApp stellt keine Netzwerkkopplung her und vermeidet so die Nachteile des VPN: Die Software schickt keine ungeprüften Abfragen und Datenpakete. Anstatt den gesamten Paketstrom des Clients filtern zu müssen, regelt CryptoApp Zugriffe auf Programmebene. So bleiben paketbasierte Angriffe, die Firewalls in heuristischen Verfahren häufig nicht erkennen, aus.

Um diesen Unterschied genauer herauszustellen, möchten wir im Folgenden Heuristiken im Gegensatz zur Senorik, die CryptoApp bieten kann, beleuchten.

2.1 Heuristik

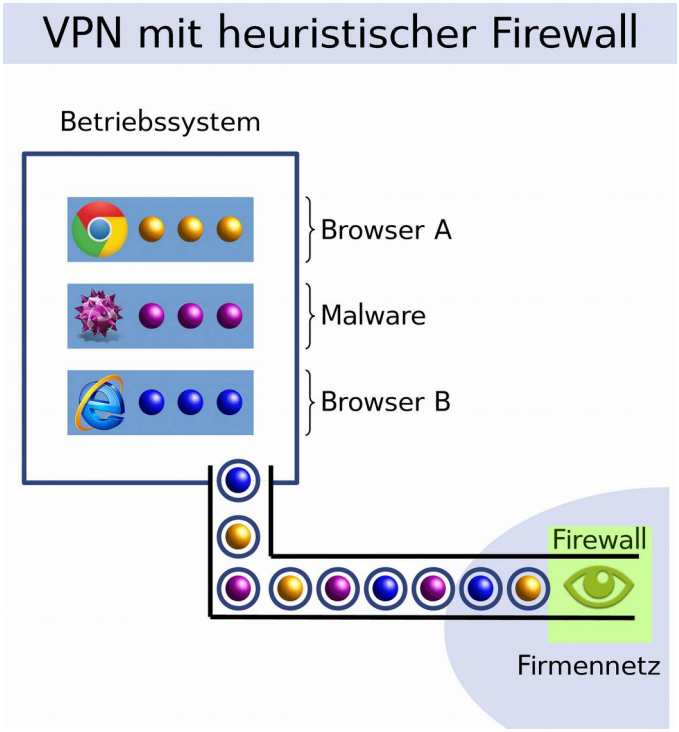
Heuristik bezeichnet die Kunst, auf Basis einer begrenzten Informationslage Aussagen zu treffen, die mit hinreichend großer Wahrscheinlichkeit richtig sind.

Der Versuch, verlässliche Aussagen zu treffen basiert auf Erfahrungen, Schätzungen, Faustregeln und zusätzlichen Hilfsannahmen. Diese Entscheidungsgrundlage kann von einem Angreifer durch einfaches Try-and-Error umgangen werden, so dass bis zu einer Veränderung der Heuristik diese nicht mehr wirksam ist. Beispielsweise gibt es heuristische Verfahren, die versuchen, Verschlüsselungstrojaner zu erkennen, indem die Zahl der bearbeiteten Dateien pro Zeiteinheit überwacht wird: Wird beispielsweise auf 30 Dateien pro Sekunde geprüft, kann die Erkennung umgangen werden, indem der Trojaner den Grenzwert aktiv nicht überschreitet.

An vielen Stellen in der IT ist es leider nicht möglich, sich eine vollständige Entscheidungsgrundlage in angemessener Zeit zu verschaffen. Stellen Sie sich einen Virenscanner vor, der ein unbekanntes Programm dekompilieren und anschließend erschöpfend analysieren soll, so dass eine belastbare Aussage getroffen werden kann: Solch eine Analyse bedeutet selbst bei kleinen Programmen einen Zeitaufwand von mehreren Tagen bevor eine Nutzung möglich ist, so dass die Nutzerakzeptanz gegen Null sinken dürfte. Während Virenscanner ein zeitliches Problem haben, stehen Firewalls vor einer ungleich größeren Herausforderung: Das Analysieren der übertragenen TCP/IP-Pakete ist zwar durchaus möglich, teils sogar auf verschlüsselte Pakete, allerdings liegen der Firewall prinzipbedingt viele Informationen nicht vor. Da alle Informationen als IP-Paket übertragen werden, kann kein Rückschluss mehr gezogen werden, welche Programme (Microsoft Office oder ein Trojaner?) tatsächlich Zugriffe tätigen und Daten übertragen.

Insbesondere in Next-Generation-Firewalls oder Intrustion-Detection/Prevention-Systemen werden immer absurder anmutende heuristische Modelle verwendet. So wird versucht, bekannte Angriffsszenarien in Zukunft beherrschen zu können. Während dieses Vorgehen von mäßigem Erfolg geprägt ist, solange Angriffe nach einem bekannten Schema ablaufen, sind neuartige Angriffe in der Regel nicht aufzuhalten. Trotz verbesserter Verfahren konnte in der letzten Dekade kein Rückgang erfolgreicher Cyber-Angriffe erreicht werden und es ist davon auszugehen – hier sei eine Extrapolation in die Zukunft erlaubt – dass dies so bleiben wird, solange IT-Security nicht vollständig neu gedacht wird.

2.2 Sensorik



Wenn Benutzer von ihren Heimarbeitsplätzen per VPN auf das Firmennetz zugreifen, stellt die VPN-Software auf dem PC, in Verbindung mit dem VPN-Gateway, eine Netzkopplung zwischen dem Betriebssystem des Rechners und dem VPN-Gateway her. In der Konsequenz können zunächst alle Programme des Client-PCs mit allen Netzwerkressourcen kommunizieren. Um dies einzuschränken und das Sicherheitsniveau zu erhöhen kommt eine Firewall zum Einsatz, die den Datenverkehr filtert und im Idealfall unerwünschte Aktionen unterbindet.

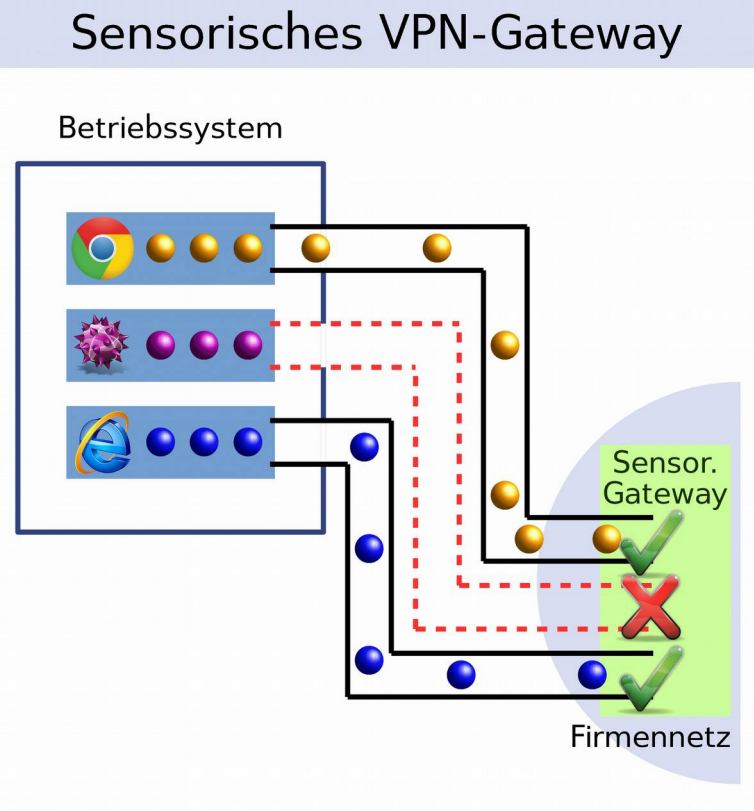
Hier kommt bereits ein wesentliches Problem zum Tragen: Der Firewall fehlen maßgebliche Informationen, die für die Entscheidung relevant sind: Beispielsweise kann die Firewall nicht wissen, welches Programm tatsächlich welche Aktion durchführen will. Es sind zahlreiche Viren bekannt, die webbasierte Systeme (z.B. ERP oder CRM-Software) im Intranet angreifen, indem sie ihren Angriff über die erlaubte Aktion „Webseite aufrufen“ durchführen. Eine Firewall kann prinzipbedingt nicht mit Sicherheit unterscheiden, ob ein Browser die Webseite aufruft, weil ein Mitarbeiter mit dem System arbeiten möchte oder ob ein Virus versucht einen Angriff durchzuführen. Für die Firewall treten in beiden Fällen nur TCP/IP-Pakete in Erscheinung, die dem Aufruf einer Webseite dienen, weshalb sie nicht blockiert werden.

Ein sensorisches System, wie dies bei CryptoApp machbar ist, wäre diesem Angriff nicht ausgeliefert, da das Gateway, welches ausschließlich die Entscheidung über die Zulässigkeit einer Kommunikation trifft zuverlässige Informationen darüber besäße, welches Programm welche Aktion durchzuführen gedenkt. In dem nur erlaubte Software freigegeben wird, kann sehr einfach sichergestellt werden, dass nur bekannte und erlaubte Programme auf erlaubte Ressourcen mit erlaubten Aktionen zugreifen können.

Versucht beispielsweise der Browser Mozilla Firefox eine Webseite aufzurufen, erhält das sensorische Gateway alle notwendigen Informationen: Welches Programm versucht welche Aktion mittels welcher Module durchzuführen?

Da nur Firefox als vertrauenswürdige Software hinterlegt ist, wird dies erlaubt. Würde allerdings ein anderer Browser oder gar ein Virus versuchen, den Webserver zu erreichen, läuft dieser Zugriffsversuch ins Leere, da weder das Virus noch der andere Browser eine Freigabe besitzen. Da in diesem Fall keinerlei Netzwerkaktionen des Virus zugelassen werden, kann dieses auch keine Analysen des Netzwerkes oder der Webserver durchführen.

2.3 Fazit



Auf den zugreifenden PCs wird ohnehin Software zum Fernzugriff ausgeführt, durch die technische Umsetzung werden dem entscheidenden System (hier der Firewall) allerdings wesentliche Informationen nicht zugänglich gemacht.

Durch eine andere Art der Zugriffssoftware, die nicht nur stumpf IP-Pakete überträgt, sondern dem Gateway, welches die Entscheidungen über die Kommunikation trifft, alle notwendigen Informationen übermittelt wird eine fundierte Entscheidungsfindung möglich. Auf diesem Weg könnte man die Schadwirkung erheblich reduzieren und die Fortpflanzung von Viren effizient unterbinden – und das nicht nur mit einer gewissen Wahrscheinlichkeit, sondern mit größtmöglicher Sicherheit.

Im Idealfall kann die Zugriffssoftware erheblich umfangreichere Informationen liefern, als nur den Programmtyp. Denkbar sind Informationen zum internen Programmauflauf und zu der Datenstruktur des jeweiligen Zugriffs.

Die Zulässigkeit eines Zugriffs kann durch die große Zahl an Informationen die das sensorische Gateway erhält anhand eines deutlich spezifischeren Regelsatzes festgestellt werden. Da dieser Regelsatz nur dem manipulationssicheren Gateway bekannt ist, kann dieser von einem Angreifer oder einer Schadsoftware nicht eingesehen oder gar manipuliert werden. Bei einem Verstoß gegen den Regelsatz – der auf einen Angriff (z.B. durch Durchprobieren) hindeutet – kann das Gateway Maßnahmen einleiten und je nach Policy und Schwere des Verstoßes unverzüglich reagieren.

Bei konsequenter Umsetzung dieses sensorischen Ansatzes lassen sich auch Intrusion-Detection-Systeme mit deutlich mehr Informationen versorgen und können so auch erheblich effektiver und mit geringerer Fehlerquote arbeiten.