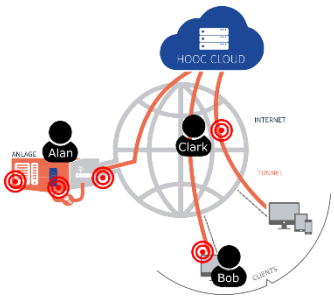
HOOC Security Paper

Bedrohungen und Massnahmen

Inhalt

Einleitung

Um über Sicherheit sprechen zu können, ist es zunächst wichtig zu wissen, woher Bedrohungen stammen können, welche Teile eines Systems angegriffen werden können, wo sich Schwachstellen befinden und welche Arten von Angriffen jeweils möglich sind.



Bedrohungen können vom Inneren eines Netzes (Alan), von einem legitimierten Benutzer im Internet (Bob) oder von einem unbekannten Dritten (Clark) ausgehen. Mögliche Ziele sind dabei unter anderem das lokale Netz bzw. Geräte im lokalen Netz, Server- und Netzwerkinfrastruktur sowie Rechner von legitimen Benutzern.

Angriffe können nun von verschiedenen Stellen aus gegen verschiedene Ziele gerichtet sein. Ohne auf Details einzugehen, seien hier einige mögliche Angriffe aufgelistet. Abhörangriffe (eavesdropping), Angreifer gibt sich als legitimierter Benutzer aus (impersonation), Ändern von Informationen während der Übermittlung (man-in-the-middle), Wörterbuchangriff auf Passwörter (brute-force bzw. dictionary attack), gezielte Überlastung der Systeme, damit diese nicht mehr erreichbar sind (denial-of-service), Einschleusen von schädlicher Software wie Viren und Trojaner (Malware) usw.

Bei herkömmlichen Methoden für den entfernten Zugriff auf Netzwerke fehlen häufig Sicherheitskonzepte, was zu einer Begünstigung von Bedrohungen führt.

Schwachstellen bei herkömmlichen Methoden für den Fernzugriff auf Netzwerke

Zugriffe auf Netzwerke durch herkömmliche Methoden wie Port-Forwarding (NAT) ermöglichen es, einzelne Dienste und Protokolle bestimmter Geräte im Netzwerk nach aussen freizugeben. Dies bringt einige Risiken mit sich:

- Firewalls bzw. Router müssen entsprechend konfiguriert und gewartet werden. Dazu ist IT-Wissen erforderlich, und die Konfiguration ist abhängig vom jeweiligen Hersteller der Geräte. Änderungen innerhalb des Netzwerkes oder der Austausch von Hardware bringen gegebenfalls Änderungen der Konfiguration mit sich.
- Die meisten Protokolle übertragen die Daten – inkl. etwaige Benutzernamen und dazugehörige Passwörter – in Klartext und können somit mitgehört und manipuliert werden.
- Die Zielsysteme sind häufig gar nicht gesichert oder nur durch Standardpasswörter, die allgemein bekannt sind. Dadurch ist eine Authentifizierung in vielen Fällen sehr einfach möglich, da keine weiteren Sicherheitsmassnahmen vorhanden sind.
- Die Zielsysteme im internen Netzwerk sind beispielsweise Wörterbuchangriffen direkt ausgesetzt und müssen damit zurechtkommen. Dies bedingt spezielles IT-Wissen, damit die Systeme entsprechend geschützt, konfiguriert und gewartet werden können.
- Ist der Zugriff auf das Zielsystem erst einmal erfolgt, kann in den meisten Fällen von dort aus so gearbeitet werden, als ob man sich direkt im Netzwerk befinden würde. Dadurch ist das meist weiter ungeschützte Netzwerk von innen bedroht.
- Eingerichtete Zugänge oder Benutzerkonten gehen gerne vergessen. Ohne entsprechende Dokumentation fehlt das Wissen, ob bestimmte Zugänge überhaupt noch benötigt werden.
- Zugangsinformationen werden oft an mehrerer Benutzer verteilt. Dadurch ist keine Kontrolle mehr möglich, wer Zugriff hat und wann jemand auf das Netzwerk zugegriffen hat.

Security und Safety der HOOC Lösung

Im angloamerikanischen Sprachraum wird zwischen den beiden Themen *Security* („Angriffssicherheit“) und *Safety* („Betriebssicherheit“) unterschieden. „Safety“ steht für den Schutz der Umgebung vor einem Objekt, also eine Art Isolation, und „Security“ beschreibt den Schutz des Objektes vor der Umgebung, d. h. die Immunität bzw. *Sicherung*. Im deutschen Sprachraum unterscheiden wir die beiden Bereiche nicht, sondern verwenden in beiden Fällen das Wort „Sicherheit“.

Unter Systemsicherheit versteht man daher eine Vielzahl von Schutzfunktionen unterschiedlicher Prägung. Wir von HOOC setzen alles daran, unsere Kunden maximal bei der Beherrschbarkeit einer Vielzahl von Einflüssen zu unterstützen. Damit ihre Anlagen, Daten und Prozesse optimal vor äusseren Einflüssen und inneren Ereignissen geschützt sind.

Vertraulichkeit (Security)

Sicherheit beim Transport Ihrer Daten – Bedrohungen von aussen

HOOC funktioniert nach einem völlig anderen Prinzip als das zuvor erwähnte herkömmliche Prinzip: Ein in einem Netzwerk installierter HOOC Gateway (bspw. HOOC Connect) verbindet sich automatisch in die HOOC Cloud. Somit kommt nie ein Verbindungsaufbau von aussen nach innen zu Stande. Die Verbindung wird mit einer 256-Bit starken AES-Verschlüsselung mit SHA-Signierung realisiert. Dieselbe Verschlüsselungstechnologie wird für den verschlüsselten Zugriff auf Webseiten verwendet und gilt als äussert sicher. Somit ist der Datenaustausch zwischen HOOC Connect und HOOC Cloud während der gesamten Übertragung sicher und für unberechtigte Dritte nicht lesbar.

Die Verbindung des HOOC Connect wird auf einem HOOC Hub terminiert. Ein HOOC Hub ist ein virtuelles Konstrukt, das wie ein physikalisches Netzwerk betrachtet werden kann. Dabei verfügt jeder HOOC Connect über einen eigenen HOOC Hub in der HOOC Cloud, wodurch die verbundenen Netzwerke immer völlig voneinander getrennt bleiben. Dadurch sind gegenseitige Zugriffe auf fremde Netzwerke niemals möglich – selbst dann nicht, wenn IP-Adressen oder andere Netzwerkinformationen bekannt sind.

Man-in-the-middle bezeichnet eine Angriffsform, bei der sich der Angreifer dem Client gegenüber als Server und dem Server gegenüber als Client ausgibt. Der „Mann in der Mitte“ hängt sich in die Kommunikation zwischen Client und Server ein und kann unbemerkt und unbehindert Daten lesen und manipulieren.

Die Verbindung zwischen HOOC Connect und seinem HOOC Hub ist vor dieser Art von Attacken geschützt. Einerseits wird die gesamte Kommunikation stets verschlüsselt, wodurch unbefugtes Lesen der Daten schon gar nicht möglich ist. Andererseits greift ein gegenseitiger, auf Zertifikaten basierter Authentifizierungsmechanismus bereits vor dem Aufbau einer Verbindung ein. Dadurch verfügt der HOOC Connect seinerseits über die Fähigkeit, die Identität eines Zielservers zu überprüfen. Handelt es sich nicht um einen Server der HOOC Cloud, wird keine Verbindung aufgebaut. Umgekehrt verfügen die Server in der HOOC Cloud über dieselben Mechanismen, um die Identitäten der HOOC Connect zu überprüfen, und lassen nur Verbindungen von bekannten HOOC Connect zu. Auch beim HOOC Connect Client kommt derselbe Authentifizierungsmechanismus wie beim HOOC Connect zum Einsatz, sodass auch hier keine Man-in-the-middle-Attacke möglich ist.

Alle eingesetzten Authentifizierungsmechanismen – sei es für die HOOC Connect und deren Clients oder für das Managementportal – sind vor Wörterbuchangriff geschützt. Treten zu viele fehlgeschlagene Anmeldeversuche innert einer gewissen Zeitspanne auf, wird der vermeintliche Angreifer durch Firewalls von der HOOC Lösung ausgeschlossen.

Identifikation (Security)

Sicherheit bei der Authentifizierung – Passwort, Mail, Account

Zur Benutzerauthentifizierung verwendet HOOC eine Kombination aus einer E-Mail-Adresse und einem Passwort. Jeder E-Mail-Adresse ist eindeutig ein Benutzerkonto zugeordnet, welches immer einer Person zugeordnet ist, die sich bei der Anmeldung entsprechend identifizieren muss. Anonyme Benutzerkonten sind bei HOOC nicht möglich. Somit wird grundsätzlich immer erreicht, dass sich beim Erteilen von Zugriffen die involvierten Parteien gegenseitig identifizieren. Vergleichen Sie dazu auch das Dokument zum Thema Supporter.

Alle verwendeten Passwörter werden von HOOC auf ihre Stärke hin überprüft und müssen bestimmten Mindestanforderungen genügen. Eigenschaften wie Passwortlänge, Verwendung von Gross- und Kleinschreibung sowie Sonderzeichen sind dabei massgebend. Je stärker ein Passwort, umso kleiner ist die Wahrscheinlichkeit, ein Passwort zufällig zu erraten oder in vernünftiger Zeit durch Wörterbuchangriffe zu finden. Starke Passwörter in Kombination mit dem oben beschriebenen Schutz vor Wörterbuchangriffen machen die Authentifizierung bei HOOC sehr sicher.

Als grosse Schwachstelle muss hier der Inhaber eines Benutzerkontos aufgeführt werden. Werden Passwörter in irgendeiner Art und Weise Dritten zugänglich gemacht, ist ein Zugriff im Rahmen der erteilten Berechtigungen uneingeschränkt möglich.

Nachvollziehbarkeit (Safety)

Wer macht was/wer hat was gemacht?

Zugriffe auf ein Netzwerk mittels HOOC Connect werden protokolliert. Damit kann nachvollzogen werden, welcher Benutzer für wie lange auf ein Netzwerk zugegriffen hat. Die auf dem Zielnetzwerk bzw. dessen Geräte getätigten Aktivitäten und Manipulationen können mit und durch HOOC nicht weiter protokoliert werden.

Die Protokollierung der verschiedenen Aktivitäten im Managementportal wird ständig ausgebaut, damit die Informationen betreffend sicherheitsrelevanten Aktionen zur späteren Einsicht bereitstehen.

Bedrohungen durch legitimierte Benutzer

Jeder legitimierte Benutzer in einem Netzwerk stellt auch eine Bedrohung dar – sei es durch Unwissenheit, Fehlmanipulationen oder Vorsatz. Daher ist es gerade bei Fernzugriffen äussert sinnvoll, über gewisse Mechanismen (bspw. Session Logs) zu verfügen, mit deren Hilfe festgelegt werden kann, welche Aktionen ein Benutzer durchführen darf und dass die Aktivitäten des Benutzer nachvollzogen werden können. Weiter kann der Zugriff auf IP Basis eingeschränkt werden.

Herkömmliche Methoden für Fernzugriffe auf Netzwerke wie das eingangs erwähnte Port-Forwarding verfügen in dieser Hinsicht in der Regel über keinerlei Funktionalität.

Unmittelbarkeit (Safety)

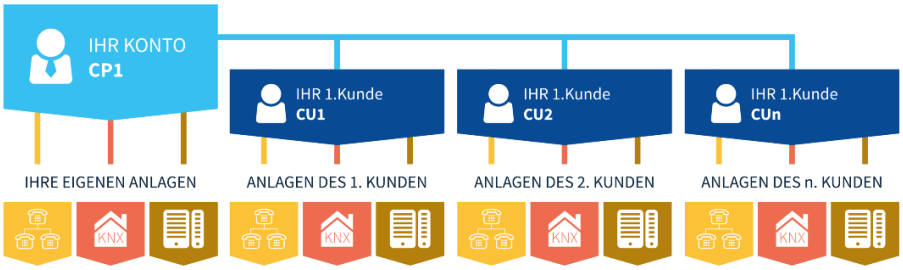
Performance und Skalierbarkeit der HOOC Cloud

Die HOOC Cloud misst und dokumentiert laufend die Auslastung und Funktionstüchtigkeit einer Vielzahl von Systemkomponenten, um bei Bedarf in sehr kurzer Zeit zusätzliche Leistung bereitstellen zu können. Dadurch kann gewährleistet werden, dass die Unmittelbarkeit von Ereignissen und Steuerinformationen gewährleistet werden kann.

Robustheit (Safety)

Wer darf was?

Dem HOOC Connect liegt für die Zugriffsverwaltung ein hierarchisches Modell zu Grunde (Siehe Abbildung), das über ein benutzerfreundliches Managementportal in der HOOC Cloud per Web-Browser verwaltet werden kann. Ein Benutzer (Reseller oder Customer) auf einer bestimmten Stufe besitzt immer die Berechtigungen für die entsprechende Stufe sowie alle darunterliegenden Stufen. Dies gilt für das Managementportal wie auch für den Fernzugriff.



Aufgrund der bei HOOC Connect zugrunde liegenden Layer-2-Tunneling-Technologie ist bei einem Fernzugriff jeweils das gesamte Zielnetzwerk erreichbar. Während dies für viele Anwendungen unabdingbar ist – und einen grossen Vorteil von HOOC Connect gegenüber anderen Lösungen darstellt –, kann dies für andere Anwendungsfälle und Anforderungen unerwünscht sein. HOOC bietet daher Netzwerkfilter an, die über das Managementportal aktiviert und konfiguriert werden können. Damit bietet sich die Möglichkeit, den gesamten Netzwerkverkehr zu blockieren und in einem weiteren Schritt den Zugriff auf bestimmte Zielgeräte bzw. deren Dienste wieder zu erlauben.

Supporter stellen eine spezielle Art von Benutzer dar, dem sehr spezifisch und über Reseller-, Customer- und Site-Grenzen hinaus Berechtigungen erteilt werden können. Dadurch wird verhindert, dass die Zugangsinformationen von Benutzerkonten an mehrere Personen verteilt werden – jeder Supporter besitzt sein eigenes, persönliches Benutzerkonto und ist dadurch identifiziert. Vergleichen Sie dazu auch das Dokument zum Thema Supporter.

Die an einen Supporter vergebenen Zugriffe können nach Belieben aktiviert bzw. deaktiviert werden und müssen gezwungenermassen zeitlich begrenzt werden. Dadurch wird verhindert, dass ein Supporter nach Wochen, Monaten oder gar Jahren immer noch unkontrollierten und vom Besitzer des Netzwerkes unbemerkten Zugriff hat.

Während ein Supporter beim Zugriff auf ein Netzwerk über die gleichen Möglichkeiten wie ein regulärer Benutzer (Reseller/Customer) bzw. wie ein Benutzer im lokalen Netzwerk verfügt, kann sein Zugriff auf das Managementportal eingeschränkt werden. Standardmässig verfügt ein Supporter auf der zugewiesenen Hierarchiestufe nur über Leserechte, während er darunterliegende Stufen auch bearbeiten kann (Schreibrechte). Dem Supporter kann durch Aktivieren des sog. Admin-Flags zusätzlich Schreibrechte für die Stufe erteilt werden, welcher der Supporter zugewiesen wurde.

Sicherheitscheckliste HOOC

Aspekt	Beschreibung	HOOC
Identifikation (Security)	Sichere Identifikation von Sender und Empfänger verhindert, dass Kommandos und Statusinformationen an falsche Adressaten gelangen bzw. solche dem System vorgegaukelt werden *(Identifikationscode, einmalige Registrierung)*	✓
Vertraulichkeit (Security)	Daten und Kommandos müssen vor der Mitverfolgung Dritter geschützt werden *(Verschlüsselung)*	✓
Verfügbarkeit (Safety)	Die Kommunikation zwischen Sender und Empfänger muss jederzeit gewährleistet sein *(Hot-Standby, Data-Backup, Self-Tests)*	✓
Nachvollzieh-barkeit (Security)	Alle Aktionen zwischen Sender und Empfänger müssen ggf. nachvollzogen werden können *(Logging)*	✓
Unmittelbarkeit (Safety)	Ereignisse und Kommandos müssen jederzeit genügend schnell ausgeführt werden können, um zeitgerecht im Sinne des Prozesses reagieren zu können *(Scalability)*	✓
Robustheit (Safety)	Sicherheit gegen Fehleingaben, Manipu-lationen und falsche, alte Daten, damit das System nicht in einen unkontrollierten Zustand gerät *(Userinterface und Prüfung durch Backend)*	✓

Schlusswort

Absolute Sicherheit gibt es keine. Ein System wird als sicher bezeichnet, wenn für einen Angreifer der Aufwand für das Eindringen höher ist als der daraus resultierende Nutzen.

HOOC realisiert die sogenannte statische Sicherheit durch geschickte Kombination verschiedener Sicherheitskonzepte, um die HOOC Lösung optimal vor Bedrohungen aus dem Internet zu schützen.

FAQ

Wo befinden sich die HOOC Cloud Server?
In zertifizierten Datenzentren in der Schweiz

Wo befinden sich meine persönlichen Daten?
Auf den Servern der HOOC Cloud, die sich in Datenzentren in der Schweiz befinden

Kann HOOC mein Passwort lesen?
Nein. Alle Passwörter werden mit der speziellen Passwort-Hash-Funktionen bcrypt unkenntlich gemacht und erst dann in die Datenbank gespeichert.

Was muss ich beim Passwort beachten?
Starke Passwörter mit einer gewissen Minimallänge, Gross- und Kleinbuchstaben, Zahlen sowie Sonderzeichen sind nötig, damit das Passwort nicht von Dritten erraten oder durch systematisches Ausprobieren gefunden werden. Die HOOC Cloud überprüft jeweils die Stärke Ihrer Passwörter und lässt schwache Passwörter gar nicht erst zu. Noch wichtiger ist jedoch, dass Sie Ihr Passwort niemals aufschreiben oder an Dritte weitergeben.

Schützt HOOC Connect mein Netzwerk vor Bedrohungen innerhalb meines Netzwerks?
Nein. HOOC Connect bietet Sicherheit für den Fernzugriff auf Ihr Netzwerk. HOOC Connect hat keinen Einfluss auf das Innere Ihres Netzwerks.

Wo liegen die Grenzen von HOOC Connect?

Es liegt in der Natur der Sache, dass von einem bestimmten Gerät des Netzwerks aus das gesamte Netzwerk manipuliert werden kann. Hier bieten sich lediglich Schutzmechanismen an, die auf dem Zielsystem laufen und entsprechend konfiguriert sind. Die HOOC Lösung bietet hierfür einzig zusätzliche Kontrolle durch das Regeln und Protokollieren des Zugangs.