Stay Untouched!

Mit dem MOBOTIX Cactus Concept zu einem rundum sicheren Videosystem

BeyondHumanVision

MOBOTIX

Die MOBOTIX AG

ist ein in Deutschland ansässiger, weltweit vertretener Entwickler und Hersteller extrem sicherer und zuverlässiger IP-Video- und Zutrittskontrollsysteme, die sowohl funktional als auch qualitativ weit über den gängigen Standards positioniert sind. Mit seinem wegweisenden Sicherheitsfokus entwickelt MOBOTIX dezentrale Technologien, die visuelle, thermale, Ton- und Sensordaten intelligent miteinander kombinieren und jeden gewünschten Bereich optimal schützen können.

Die MOBOTIX Lösungen sind dabei anwenderorientiert auf intuitive Bedienbarkeit ausgelegt. Selbst komplexe Problemstellungen in Handel, Bildung, Gesundheits- und Verkehrswesen, Mobilität und Gastronomie lassen sich so leichter bewältigen. MOBOTIX Produkte bieten ein exzellentes Kosten-Nutzen-Verhältnis über die gesamte Nutzungsdauer. Technisch verzichtet MOBOTIX auf mechanische, wartungsanfällige Komponenten und nutzt serienmäßig die branchenweit besten Sicherheitskomponenten. Die jahrelange Nutzbarkeit eines MOBOTIX Produkts wird durch regelmäßige Software-Upgrades mit neuen Funktionen und Sicherheitsverbesserungen unterstützt.

Cybersicherheit auch grundlegend für Videosicherheitssysteme

Videoüberwachung sorgt für Sicherheit und schützt so Tag für Tag Milliarden von Menschen. Familien können ihren Wochenendeinkauf unter dem schützenden Auge von Kameras erledigen, und besorgte Eltern behalten ihr schlafendes Kind im Blick. So spielt die Videoüberwachung für uns alle eine wichtige Rolle. Weltweit hat unser Netzwerk aus zertifizierten Partnern in 150 Ländern mehr als eine Million MOBOTIX Kameras installiert.

Dank ihrer zahlreichen Vorteile sind Videosicherheitssysteme inzwischen zu einer beliebten Zielscheibe für Kriminelle und Terroristen geworden. Früher waren Angriffe auf Videosicherheitssysteme eine Seltenheit. Schließlich handelte es sich meist um geschlossene, in Privatbesitz befindliche Systeme, die direkt mit einer Leitstelle vor Ort verkabelt waren. Die Zeiten haben sich jedoch grundlegend geändert. Moderne Videokameras sind im Grunde Computer, die eine mit einer Videokamera verbundene Software ausführen.

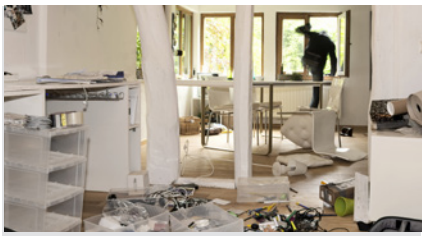
Risiken durch Cyber-Attacken:

- Wachsende Angriffsfläche durch immer mehr IP-Geräte
- Deaktivierung und Fernsteuerung
- Abgreifen von Daten
- Übernahme und Zweckentfremdung von Geräten
- Industrielle und staatlich geförderte Spionage
- Aussperren durch Ransomware-Angriffe

Dank der Ausbreitung des Internets und gesunkener Anschaffungskosten sind Videosicherheitssysteme zunehmend über IP-Netzwerke zugänglich. Dadurch ist aber zugleich die Gefahr von Hackerangriffen gestiegen.

Mögliche Schäden

Kriminelle Hackerangriffe auf Videosicherheits- und Zutrittskontrollsysteme können Leben kosten und auch sonst immense Schäden verursachen. Aus Versicherungsgründen muss in einigen Bereichen heute zwingend ein Videosicherheitssystem installiert sein. Wird dieses jedoch aufgrund eines vermeidbaren Hackerangriffs lahmgelegt und dann eine Straftat begangen, die nicht mehr von der Kamera festgehalten wird, können Entschädigungszahlungen wegen Verstoßes gegen die Versicherungsbedingungen verweigert werden.



Potenzielle Schäden:

- Finanzielle Verluste und Imageschäden
- Regulierungsmaßnahmen, Bußgelder und strafrechtliche Verfolgung aufgrund fahrlässigen Handelns
- Vertragsverletzungen, Zivil- und Sammelklagen
- Verlust von Menschenleben durch gezielte Terroranschläge

Doch die Absicherung von Videoanlagen berührt auch datenschutzrechtliche Fragen. In den meisten Staaten müssen heute personenbezogene Daten zu Gesundheit, Finanzen, politischer Gesinnung und anderen Kriterien grundsätzlich sicher erfasst und gespeichert werden. Das gilt auch für Videodaten und betrifft beispielsweise Personen, die an einer politischen Kundgebung teilnehmen. Stets ist das Bildmaterial sicher und für Dritte unzugänglich aufzubewahren. Im Falle eines Cyberangriffs auf das Videosystem besteht ein hohes Risiko, dass personenbezogene Bilder und andere Daten, anhand derer bestimmte Personen identifiziert werden können, gestohlen und unbefugt offengelegt werden. Dies würde die Datenschutzrechte der überwachten Personen verletzen und könnte rechtliche Konsequenzen für die Systemverantwortlichen nach sich ziehen.

In allen betroffenen Bereichen gilt, dass nachweisliche Fahrlässigkeit zu Rufschädigungen, aufsichtsrechtlichen Konsequenzen, Geldstrafen und sogar Strafverfahren führen kann. In zivilrechtlicher Hinsicht können wegen Vertragsbruchs Zivil- und Sammelklagen die Folge sein.

Wettbewerbsposition

Videosicherheits- und Zutrittskontrollvorrichtungen gehören einer Technikkategorie an, die als Internet der Dinge (IoT – Internet of Things) bezeichnet wird. Technologieunternehmen und Analysten wie Gartner, Cisco und andere gehen davon aus, dass bis zum Jahr 2020 bis zu 50 Millionen solcher IoT-Geräte im Einsatz sein werden (Quelle: www.cisco.com). Im Gegensatz zu Radiosendern, Fernsehsendern und Kraftfahrzeugen bewegt sich die IoT-Technik noch in einer rechtlichen Grauzone. Bislang existieren keine verbindlichen Standards für die Sicherung entsprechender Geräte. Aktuell wird die Technologie jedoch in zunehmendem Maße autonom. Damit steigt das Risiko, dass ungesicherte Geräte – ähnlich wie bislang Desktop-PCs – massenhaft Viren anziehen, welche dann wiederum in Videosicherheitssysteme eindringen, wo sie nur schwer erkannt und beseitigt werden können.

„Mirai"-Botnet-Angriffe, 2016
Erstmals IP-Kameras betroffen

Beispiele geschädigter Server:

9/2016	Minecraft, OHV
10/2016	Dyn
11/2016	(U.S. Präsidentschaftswahl): Twitter, Spotify, Amazon
11/2016	Libysche Regierung
11/2016	Deutsche Telekom

Ein Fallbeispiel aus der Praxis

Oft werden Hackerangriffe auf Videosicherheitsanlagen weder erkannt noch gemeldet. Werden Geräte jedoch von außen gekapert und dann für Angriffe auf andere Internet-Anwendungen genutzt, lässt sich das Problem kaum noch ignorieren. Für eine Attacke wie im Herbst 2016, von der Twitter, Amazon, Tumblr, Reddit, Spotify und Netflix betroffen waren, zeichneten in Teilen Videosicherheitsgeräte verantwortlich, die zuvor von Hackern übernommen worden waren. Das Botnet bestand primär aus digitalen

Videorekordern und IP-Kameras einer chinesischen Hightechfirma. Diese liefert jedoch auch Komponenten an zahlreiche andere Videohersteller. Zehntausende dieser Geräte sind nun zu gefährlichen Waffen im Cyberkrieg umfunktioniert worden.

Das MOBOTIX Cactus Concept

Als Antwort auf solche Problemstellungen hat MOBOTIX eine Cybersicherheitsstrategie unter dem Titel „Cactus Concept“ entwickelt, mit der die Produkte von MOBOTIX umfassend vor Hackerangriffen geschützt werden.

Der Kaktus versinnbildlicht dabei den Kerngedanken hinter der MOBOTIX Strategie, bei der jede einzelne Hardware- und Software-Komponente mehrfach gegen externe Bedrohungen abgesichert wird.

Ähnlich den Dornen und der Widerstandsfähigkeit von Kakteen verwendet MOBOTIX eine lückenlose End-to-End-Verschlüsselung – von der Bildquelle über die Datenkabel und -speicher bis hin zum Video-Managementsystem auf dem Computer des Nutzers. Und wie bei einem Kaktus, der vollständig mit Dornen geschützt ist, verfügen alle Module einschließlich Kamera, Speicher, Kabel und Video-Managementsystem im MOBOTIX System über digitale „Dornen“, die sie vor unbefugtem Zugriff schützen

Dennoch sind Sicherheitstechnologien immer nur dann erfolgreich, wenn die Benutzer die vorhandenen Systeme richtig bedienen. Ein weiteres Ziel des Cactus Concept ist es daher, potenzielle und bestehende Kunden von MOBOTIX über die Bedeutung von Datensicherheit in netzwerkbasierten Videosicherheitssystemen aufzuklären und ihnen zu zeigen, wie Unternehmen sich mithilfe von kosteneffizienten und intelligenten Lösungen optimal schützen können.

Die Bestandteile des Cactus Concept

MOBOTIX nimmt innerhalb der Branche eine Sonderstellung ein, da das Unternehmen seine gesamte Software selbst entwickelt, anstatt Entwicklungen anderer Hersteller zu lizenzieren. Dieser innovative Ansatz bietet beträchtliche Sicherheitsvorteile. Da die gesamte Software-Entwicklungskette in Unternehmenshand liegt, ist MOBOTIX weniger anfällig für die Schwachstellen als andere Marken, bei denen unausgereifte Software und Hardware von Drittanbietern Sicherheitsprobleme verursacht. Das Cactus Concept steht für „Sicherheit von Haus aus“, ist von Beginn an im Unternehmen eingebettet und in sämtlichen Bereichen erkennbar.

Der Kaktus:

Wächst in rauen Umgebungen

Äußerst genügsam

Sehr robust

Wird sehr alt

Geschützt durch Stacheln

CYBER SECURITY INITIATIVE

Eigene Entwicklung garantiert sichere Software

Die Sicherheitsphilosophie von MOBOTIX setzt bereits im Betriebssystem und im Application Stack an. Alle MOBOTIX Geräte arbeiten auf Basis eines modifizierten Linux-Betriebssystems, das auf nicht benötigte Standarddienste und -module verzichtet. Stattdessen wurden kritische Linux-Module, wie die Authentifizierung, komplett umgestaltet. So kann MOBOTIX sicherstellen, dass diese Module nicht für gängige Exploits oder Code-Injection-Techniken anfällig sind. Das

Betriebssystem ist nicht quelloffen und wird durch zusätzliche, softwarebasierte Sicherheitsmechanismen geschützt. Zudem ist jedes Update für Geräte-Firmware und Softwarekomponenten verschlüsselt und digital signiert, um Manipulation vorzubeugen.

Geräte- und Kommunikationssicherheit

Alle Aufzeichnungen, die von der Kamera generiert werden, werden vor der Speicherung schon im Gerät selbst verschlüsselt – angefangen vom Ringpuffer, der die in jede Kamera integrierte SD-Karte nutzt. MOBOTIX hat ein sicheres Dateisystem entwickelt. Wenn eine Kamera gehackt oder gestohlen wird, kann der Zugriff auf kameraintern aufgezeichnete Videodaten verweigert werden, wenn keine Administratorrechte vorliegen, die wiederum mithilfe der zuvor beschriebenen Konfigurationsprozesse geschützt werden. Jedes MOBOTIX Gerät kann darüber hinaus mit Diebstahl- und Manipulationssicherungen wie verstärkten Gehäusen, Sensoren, Alarm- und Warnfunktionen genutzt werden.

Der Zugriff auf die Bedienschnittstelle zur Kamerakonfiguration ist nur autorisierten Anwendern gestattet. In jedem System können abgestufte Rechte für verschiedene Benutzergruppen erstellt werden. Das bedeutet in der Praxis: Kameras von MOBOTIX speichern Anwenderpasswörter niemals als Klartext, sondern versehen diese mit einem komplexen Hash-Algorithmus (SHA-512). Gelangt eine Konfigurationsdatei in falsche Hände, wäre es extrem schwierig, das Passwort im Klartextformat zu extrahieren. Nicht benötigte Dienste werden deaktiviert, um potenzielle Schwachstellen zu beseitigen und Angriffen vorzubeugen. Zudem gibt es kein undokumentiertes Master-Passwort – Kameras von MOBOTIX können ausschließlich über ihre grafische Benutzeroberfläche (Web GUI) angesteuert und konfiguriert werden.

Sichere Netzwerk- und Gerätekommunikation

Alle zwischen MOBOTIX Kameras und anderen Netzwerk-Hosts ausgetauschten Daten können verschlüsselt werden, um die Vertraulichkeit und Integrität der Datenströme zu gewährleisten. Dieselbe Technologie, mit der Onlinebanking per HTTPS gesichert wird (SSL/TLS), sowie digitale Stammzertifikate werden in Einklang mit bewährten Verfahren standardmäßig unterstützt.

MOBOTIX bietet zudem integrierte Unterstützung zur Verwaltung eindeutiger X.509-Zertifikate auf jeder Videoquelle, damit Unternehmen Kameras und Türstationen sichern können, die über Systeme wie OpenVPN authentifiziert werden. Das bedeutet: Wird eine Kamera gestohlen oder gehackt, kann der Angreifer mit den Zugriffsdaten der kompromittierten Kamera nicht das übrige Kamerasystem infiltrieren.

Kontinuierliche Überprüfung und Kontrolle

Trotz alledem müssen diese Verfahren überprüft werden, um die Sicherheit der Umgebung zuverlässig gewährleisten zu können. Dazu nimmt MOBOTIX die Dienste der SySS GmbH (www.syss.de) in Anspruch, einem angesehenen und unabhängigen Anbieter für externe Penetrationstest, der die Sicherheit sowohl von Software- als auch Hardwarekomponenten eingehend prüft und zertifiziert. Das Prüfverfahren beinhaltet umfassende Systempenetrationstests, bei denen versierte Hacker versuchen, die einzelnen Schutzmechanismen zu überwinden. So können etwaige Lücken geschlossen werden, noch bevor die Produktion beginnt.

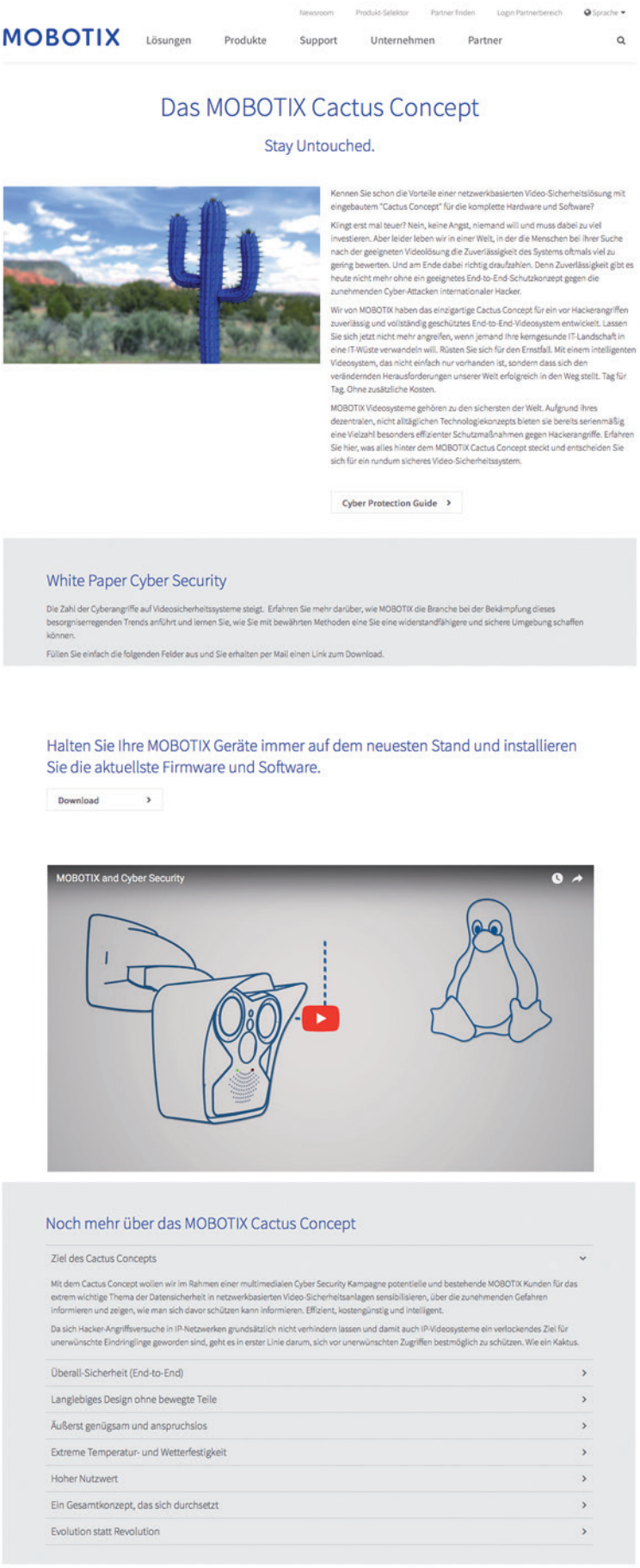
Stay untouched – mit MOBOTIX

Die Beliebtheit der Videoüberwachung wächst und damit auch für die Gefahr von Hackerangriffen. Deshalb schützt MOBOTIX seine Geräte aktiv vor Bedrohungen. Unser Cactus Concept zielt darauf ab, potenzielle und bestehende Kunden von MOBOTIX über die besondere Bedeutung von Datensicherheit in netzwerkbasierten Videosicherheitssystemen aufzuklären.

Wir unterstützen unsere Kunden dabei, die Cybersicherheit ihrer Umgebung kontinuierlich zu erhöhen. Da überlegene Sicherheit ein Eckpfeiler des MOBOTIX Wertversprechens ist, streben wir die Zusammenarbeit mit anderen Branchenakteuren, Kunden und Behörden an, um Technologien und Systeme zu schützen, die unsere Gesellschaft zu einem sichereren Ort für uns alle machen.

Weitere Informationen zum Thema Cybersicherheit erhalten Sie unter:

www.cactusconcept.com



BeyondHumanVision

Wir heben uns nicht durch eine besondere Funktion oder ein bestimmtes Designelement ab.

Das Alleinstellungsmerkmal von MOBOTIX ist unser Gesamtpaket aus Technologie, Innovation und Qualität, mit dem wir eine Komplettlösung bereitstellen. Wir kombinieren jedes Element und bieten damit höchste Flexibilität sowie ein hochtechnisiertes Tool-Set, mit dem Sie reale Probleme so effizient und zuverlässig wie möglich lösen können.

Wir bei MOBOTIX sehen über die menschliche Perspektive hinaus, um Sie heute zu unterstützen und auf die Zukunft vorzubereiten.

DE_03/18

MOBOTIX AG

Kaiserstrasse
D-67722 Langmeil
Tel.: +49 6302 9816-104
Fax: +49 6302 9816-190
www.mobotix.com

MOBOTIX