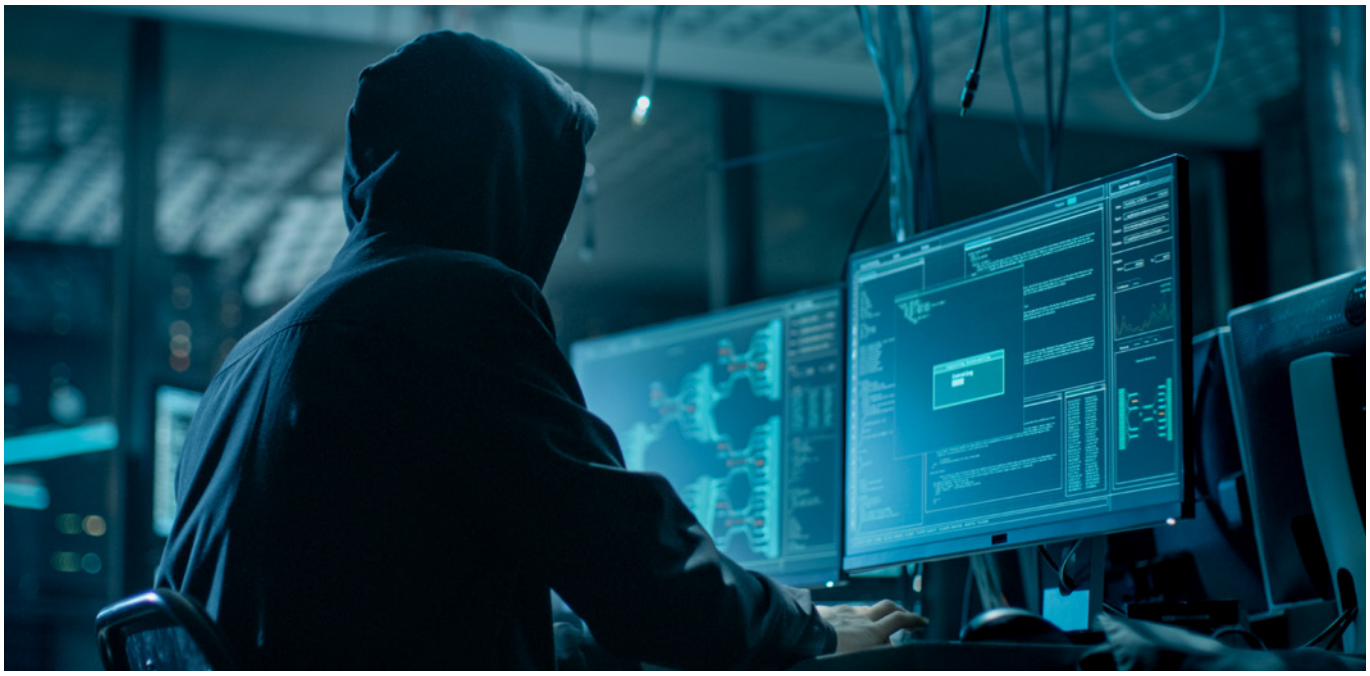
# Tecnologia a prova di violazione!

Scopra il “concetto Cactus” di MOBOTIX contro i rischi cibernetici per il suo sistema di videosorveglianza

Rappresentato da:

BeyondHumanVision

MOBOTIX



## Introduzione - Chi è MOBOTIX?

MOBOTIX sviluppa e produce sistemi di controllo degli accessi e video IP a sicurezza elevata che vanno oltre la visione umana. Concentrandoci sulla sicurezza e andando oltre, MOBOTIX ha spianato la strada grazie alla tecnologia decentralizzata intelligente, che combina dati visivi, termici, acustici e dei sensori al fine di proteggere meglio ogni tipologia di ambiente.

Concepite per un uso intuitivo e grazie al supporto dell’intelligenza artificiale, le soluzioni MOBOTIX contribuiscono a risolvere le problematiche più insidiose nei settori retail, formazione, assistenza sanitaria, trasporti, mobilità e ospitalità. I prodotti MOBOTIX sono progettati senza parti mobili e vantano sistemi di controllo per la sicurezza cibernetica all’avanguardia in grado di offrire il miglior ritorno complessivo degli investimenti. Un ciclo operativo di durata straordinaria viene garantito e consolidato dai costanti aggiornamenti software.

## Perché la sicurezza cibernetica è così importante per i sistemi di videosorveglianza?

La videosorveglianza è garanzia di sicurezza e aiuta miliardi di persone ogni giorno. Che sia una famiglia in un centro commerciale protetto dall’occhio di una telecamera di videosorveglianza, o una coppia di genitori che controlla un neonato mentre dorme: la videosorveglianza riguarda tutti noi. In tutto il mondo, in effetti, sono state installate oltre un milione di telecamere MOBOTIX sfruttando una rete di partner certificati distribuiti su 150 paesi.

Sono tutti questi vantaggi ad aver attirato l’attenzione dei criminali, che ora tentano di attaccare i sistemi di videosorveglianza. Gli attacchi alle reti di videosorveglianza in passato erano fenomeni rari grazie ai sistemi chiusi, spesso collegati direttamente alle sale di controllo locali tramite reti private cablate. Tuttavia, i tempi cambiano e le telecamere moderne sono diventate computer performanti, dotate di software collegati a una videocamera. Con l’avvento di Internet e di telecamere più a buon mercato, i sistemi di videosorveglianza ora risultano molto più accessibili da una rete IP, causando l’aumento dei potenziali attacchi cibernetici.

**Rischi degli attacchi cibernetici:**

- Il numero crescenti di dispositivi IP amplia la base d’attacco
- Disattivazione e controllo remoto
- Raccolta dei dati
- Acquisizione e abuso dei dispositivi
- Spionaggio industriale e finanziato dai governi
- Accesso bloccato dagli attacchi ransomware

## Danni potenziali

Un attacco cibernetico ben eseguito contro i sistemi di videosorveglianza e di controllo

degli accessi può portare a potenziali vittime e ulteriori danni notevoli causati da attacchi portati a termine in modo più mirato e profondo. Inoltre, mentre i sistemi di videosorveglianza diventano sempre più un obbligo per determinate sedi professionali o vengono inclusi nella copertura assicurativa, nel caso in cui un sistema di videosorveglianza diventi non operativo a causa di un attacco cibernetico evitabile e in quel momento venga commesso un crimine non ripreso dalla telecamera, i gestori dell'assicurazione potrebbero rifiutarsi di dare seguito alle richieste per non aver ottemperato ai termini del rilevamento video.

**Danni potenziali:**

- Perdite economiche e danno d'immagine
- Misure correttive, sanzioni e procedimento legale per negligenza
- Violazioni contrattuali, richieste di risarcimento danni
- Perdita di vite umane a causa di attacchi terroristici mirati

Le reti protettive di videosorveglianza, inoltre, sollevano questioni legate alla sfera privata. La maggior parte dei governi esige ora che tutti i dati personali di natura privata pertinenti alle aree sanità, finanza, affiliazione politica, uniti a una serie di altri criteri, debbano essere archiviati con una modalità sicura. Questo riguarda anche i dati video. Un individuo che partecipa a una manifestazione politica, per esempio, si aspetta che qualsiasi filmato di videosorveglianza sia conservato al sicuro e lontano dal dominio pubblico. Nel caso di un attacco informatico contro un dispositivo o una rete di videosorveglianza, c'è un rischio molto elevato che informazioni personali come immagini e altri dati in grado di far risalire a persone specifiche possano essere rubati e diffusi senza autorizzazione. Questa operazione violerebbe il diritto alla privacy degli utenti monitorati dal sistema e potrebbe celare conseguenze legali per la persona considerata responsabile del trattamento dei dati.

In tutte queste aree, qualora sia possibile provare un comportamento negligente, si prefigurano potenzialmente un danno catastrofico in termini di reputazione, oltre a misure correttive, sanzioni e procedimenti penali. In questioni civili, sono possibili violazioni contrattuali, azioni legali civili e class action.

## La posizione dell'industria

I dispositivi di videosorveglianza e di controllo degli accessi rientrano nella categoria di tecnologie denominata Internet degli oggetti (da Internet of Things, IoT). Le società e gli analisti tecnologici quali Gartner, Cisco e altri prospettano che entro il 2020 verranno utilizzati fino a 50 miliardi di dispositivi IoT (fonte: www.cisco.com). Diversamente dalle emittenti radio, dalle stazioni TV o dai veicoli a motore, la legislazione in materia di ciò che può essere connesso a Internet è quasi assente. Non sono presenti standard obbligatori circa il grado di sicurezza che deve possedere un oggetto. Tuttavia, mentre la tecnologia aumenta il proprio livello di automazione, il rischio che i dispositivi non sicuri attraggano i virus in forma pandemica, come era successo per gli utenti dei PC desktop, potrebbe iniziare a ricomparire, ad esempio nelle reti delle telecamere di videosorveglianza. In questi casi le modalità per rilevare o arginare rapidamente il problema sono ridotte.

**Attacco botnet "Mirai", 2016**
Per la prima volta colpite anche le telecamere IP

Esempi di server danneggiati:

| | |
|---|---|
| 9/2016 | Minecraft, OHV |
| 10/2016 | Dyn |
| 11/2016 | (Elezioni presidenziali americane): Twitter, Spotify, Amazon |
| 11/2016 | Governo della Liberia |
| 11/2016 | Deutsche Telekom |

## I problemi del mondo reale

Gli attacchi informativi contro gli apparecchi di videosorveglianza spesso non vengono rilevati o segnalati. Tuttavia, se tali dispositivi vengono acquisiti e utilizzati per sferrare attacchi ad altre risorse di Internet, la questione non è più ignorabile. Un impressionante attacco di questo genere nell'ottobre 2016 che ha interessato Twitter, Amazon, Tumblr, Reddit, Spotify e Netflix è stato generato in parte da una rete di dispositivi di videosorveglianza acquisiti mediante un attacco cibernetico. Il botnet è formato principalmente dai videoregistratori digitali (DVR) e dalle telecamere IP prodotte da un'a-

zienda cinese di alta tecnologia. I componenti prodotti sono venduti ai fornitori che li usano nei propri prodotti, causando decine di migliaia di cooptati all’interno di queste pericolose armi cibernetiche.

# Introduzione Il “concetto cactus” di MOBOTIX

In risposta a tali problematiche, MOBOTIX ha creato una strategia di sicurezza informatica denominata “Concetto Cactus” che mira ad offrire un approccio esaustivo per la protezione dei prodotti MOBOTIX dalle minacce legate agli attacchi cibernetici.

Il cactus simboleggia l’idea di base che si cela dietro la strategia per la sicurezza informatica di MOBOTIX, in cui ciascun componente hardware e software viene protetto mediante una serie di meccanismi di difesa destinati ad arrestare le minacce esterne.

Prendiamo ad esempio le spine e la spessa superficie del cactus: MOBOTIX ricorre alla crittografia end-to-end senza punti ciechi, dalla sorgente dell’immagine attraverso i cavi dati e la memoria fino al sistema di gestione video sul computer dell’utente. Proprio come un cactus, coperto di spine in ogni sua parte, così tutti i moduli del sistema MOBOTIX (videocamera, memoria, cavi e sistema di gestione video) hanno spine digitali che li proteggono dagli accessi non autorizzati.

Le tecnologie per la sicurezza, tuttavia, hanno un’efficacia pari a quella del processo che l’utente utilizza per gestire questi sistemi. A tale proposito, un ulteriore obiettivo del progetto “Cactus Concept” è incrementare, tra i clienti esistenti e potenziali di MOBOTIX, la consapevolezza dell’importante problema della sicurezza dei dati nei sistemi di videosorveglianza basati sulla rete e del modo in cui le organizzazioni possono proteggersi attraverso soluzioni intelligenti e convenienti sotto il profilo dei costi.

## Gli elementi del concetto cactus

MOBOTIX si contraddistingue nettamente nel proprio settore, in quanto sviluppa tutti i propri software in-house e non concede la propria tecnologia in licenza a terze parti.

**Il cactus:**

Cresce in ambienti critici

È molto economico

È molto robusto

Ha una durata elevata

È protetto dalle spine

Tale approccio all’avanguardia implica vantaggi significativi quando si tratta di sicurezza. Controllando l’intera sequenza di sviluppo del software, MOBOTIX è meno vulnerabile agli attacchi di terze parti che hanno coinvolto gli altri marchi in cui una vulnerabilità dei software e hardware esterni causa problemi di sicurezza. Il Concetto Cactus è una “sicurezza come filosofia aziendale di progettazione” che ci caratterizza dal primo giorno ed è evidente in molteplici aree.

CYBER SECURITY INITIATIVE

## Software e sviluppo sicuri

Il concept di sicurezza MOBOTIX inizia all’interno della fase di progettazione che interessa sistema operativo e stack applicativo. Tutti i dispositivi MOBOTIX si basano su un sistema operativo Linux modificato e sicuro che rimuove i servizi e i moduli standard. Invece, i moduli Linux critici come l’autenticazione sono stati completamente riprogettati dagli esperti MOBOTIX per garantire che non siano vulnerabili ad exploit degli standard o a tecniche di aggressione tramite iniezione di codici. Questo sistema operativo non è open source ed è protetto da software

di sicurezza supplementari. Ogni aggiornamento del firmware del dispositivo e degli elementi software, inoltre, è criptato e dotato di firma digitale per impedire manomissioni.

## Sicurezza dei dispositivi e comunicazione sicura

Tutte le registrazioni create dalla telecamera vengono criptate internamente prima dell'archiviazione, iniziando dalla memoria circolare che utilizza la scheda SD integrata in ciascuna telecamera. MOBOTIX ha realizzato un file system sicuro nell'ipotesi che una telecamera venga effettivamente rubata o hackerata: i video precedentemente registrati ancora presenti nella telecamera non potranno essere recuperati senza prima ottenere i diritti di amministratore protetti tramite i processi di configurazione sicura descritti precedentemente. Ciascun dispositivo MOBOTIX può inoltre essere dotato di meccanismi antifurto e anti-manomissione, tra cui involucri rinforzati, funzioni dedicate a sensori, allarmi e avvisi.

L'accesso all'interfaccia di configurazione della telecamera viene concesso solo agli utenti autorizzati. Per garantire la sicurezza interna, ciascun sistema consente la creazione e l'implementazione di diritti diversi per gruppi di utenti diversi. In pratica questo significa che le telecamere MOBOTIX non memorizzano mai le password utente con testo in chiaro, bensì vengono crittografate con un potente algoritmo di hashing unidirezionale (SHA-512) in modo che se il file di configurazione dovesse finire in mani sbagliate, risulterebbe estremamente difficile recuperare la password in chiaro. I servizi non essenziali vengono disabilitati per limitare i potenziali exploit e prevenire gli attacchi. Inoltre non è presente alcuna "master password" non documentata: l'unico modo per accedere e configurare una telecamera MOBOTIX è tramite la propria GUI web (Graphical User Interface).

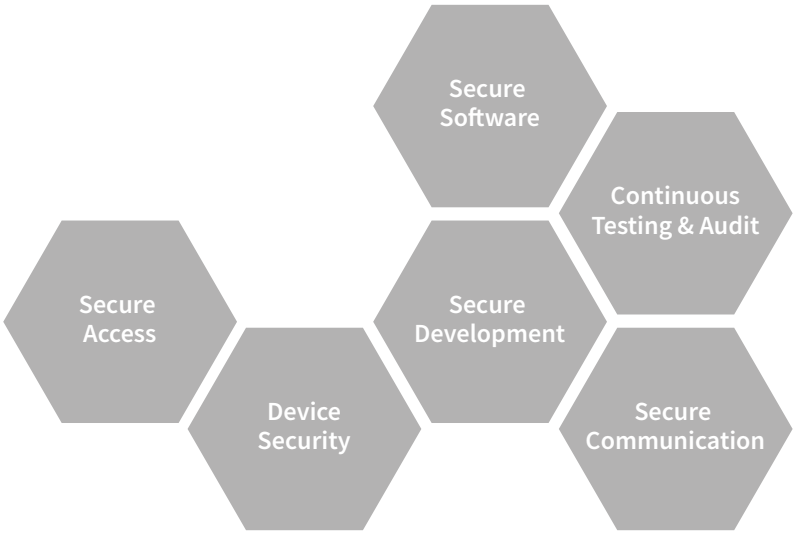
## Rete sicura e comunicazione del dispositivo

Tutti i dati scambiati tra le telecamere MOBOTIX e gli altri host nella rete possono essere criptati per garantire riservatezza e integrità dei dati in transito. La medesima tecnologia impiegata per proteggere gli HTTPS dei siti di banking su Internet (SSL/TLS) e i certificati digitali sono tutti supportati come standard per soddisfare le linee guida delle buone pratiche previste dalle maggiori strutture di sicurezza degli esperti.

MOBOTIX inoltre include il supporto integrato per la gestione dei certificati unici X.509 in ciascuna telecamera e delle Root Certificate Authorities per consentire alle imprese di ampliare la sicurezza dei dispositivi includendo telecamere e videocitofoni autenticati tramite sistemi come OpenVPN. Questo significa che qualora una telecamera venga effettivamente rubata o hackerata, l'aggressore non potrà usare le credenziali in una telecamera compromessa per attaccare la rete residua di telecamere.

## Valutazioni costanti e controllo

Tuttavia, tutti questi provvedimenti devono essere convalidati come garanzia di un ambiente effettivamente sicuro. Al fine di garantire tale sicurezza, MOBOTIX si avvale dei servizi di SySS (www.syss.de), una società terza indipendente ed estremamente affidabile nel campo della valutazione della sicurezza informatica, che analizza la sicurezza degli elementi software e hardware. La valutazione spazia sino a test completi di penetrazione in cui dei team di hacker esperti cercano di aprire una breccia nei nostri sistemi di controllo, così da consentirci di rimediare a qualsiasi problematica prima di arrivare alla fase di produzione.



# Tecnologia a prova di violazione con MOBOTIX

La popolarità legata alla videosorveglianza è in aumento tanto quanto le minacce provenienti dagli attacchi cibernetici. MOBOTIX protegge attivamente i propri dispositivi da questi rischi e il nostro concetto cactus mira a incrementare, tra i clienti esistenti e potenziali di MOBOTIX, la consapevolezza del problema estremamente importante della sicurezza dei dati nei sistemi di videosorveglianza basati sulla rete.

Fornendo gli strumenti in grado di contribuire alla creazione di ambienti più sicuri per i nostri clienti, oltre all’impegno volto a rendere la sicurezza una parte fondamentale del concetto di valore di MOBOTIX, puntiamo a collaborare con le altre aziende del nostro settore, i clienti e gli organismi di governo per proteggere i dispositivi tecnologici e i sistemi che rendono la società più sicura per tutti..

Per ulteriori informazioni, visiti la pagina del Concetto Cactus al seguente sito web:

**www.cactusconcept.com**

# BeyondHumanVision

## Il nostro punto di forza esclusivo non è una singola caratteristica o un singolo elemento progettuale.

Con MOBOTIX, il nostro punto di forza esclusivo è il pacchetto totale che riunisce tecnologia, innovazione e qualità per offrire una soluzione completa. Attraverso la combinazione dei singoli elementi, siamo in grado di offrire la massima flessibilità grazie a una serie di strumenti tecnologicamente avanzati che consentono di risolvere problemi concreti nel modo più efficiente ed affidabile.

Con MOBOTIX, andiamo oltre la visione umana per aiutarla oggi a prepararsi per il futuro

**IT_05/18**

**MOBOTIX AG**

Kaiserstrasse
D-67722 Langmeil
Tel.: +49 6302 9816-103
Fax: +49 6302 9816-190
www.mobotix.com

MOBOTIX