IXON Security Guide

IXON Cloud I Security Guide

Ultimo aggiornamento: 14/05/2024

Prefazione

Questa guida è pensata per i costruttori di macchine che integrano i prodotti IXON nelle loro macchine e per le aziende che utilizzano questi sistemi connessi.

Per IXON, la sicurezza informatica è la massima priorità. Riteniamo che la trasparenza stia alla base di una sicurezza informatica efficace ed è per questo che non intendiamo nascondere dettagli o fornire informazioni incomplete. La nostra mission è collaborare con i costruttori per fare in modo che le loro macchine siano al sicuro. È quindi fondamentale che il costruttore abbia accesso a informazioni dettagliate sulle procedure interne di IXON.

La sicurezza informatica è un argomento molto ampio e non è semplice gestirlo a un livello che sia alla portata di tutti. Questa guida vuole quindi fornire dettagli accurati sul nostro approccio alla sicurezza a diversi livelli, trattando tutti gli aspetti di IXON, i nostri prodotti e le linee guida per il loro sviluppo sicuro.

Come sempre, siamo qui per aiutarvi. Se qualcosa non è chiaro o non viene trattato, scriveteci all'indirizzo security@ixon.cloud.

Dylan Eikelenboom,
Security Officer di IXON

Indice

.

Criminalità informatica nel settore manifatturiero

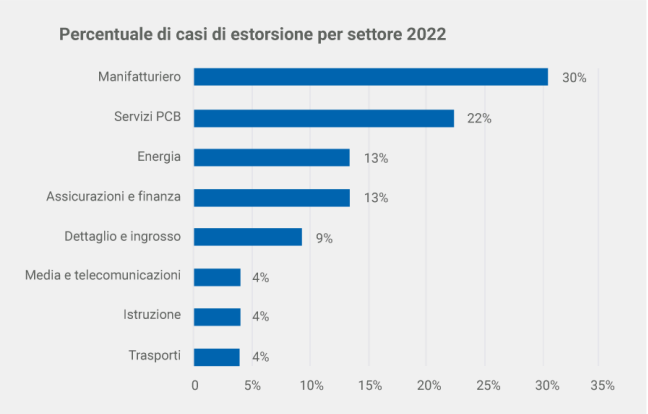
La criminalità informatica è una delle minacce principali alle industrie di tutto il mondo. Il settore manifatturiero è particolarmente vulnerabile ed è diventato uno degli obiettivi principali dei criminali informatici. Con l'integrazione di un maggior numero di tecnologie nelle linee produttive e nei processi industriali, aumenta anche l'esposizione all'attacco. Ora più che mai, i responsabili degli stabilimenti devono essere attenti quando introducono nuovi macchinari nel loro ambiente.

Ransomware: un rischio importante per i produttori

Uno dei rischi di sicurezza per le macchine è il ransomware, che cripta i dati aziendali e richiede un riscatto per liberarli. Questa forma di crimine informatico può bloccare la produzione, causare perdite finanziarie significative e danneggiare la reputazione. Data la natura della produzione in termini di uptime e proprietà intellettuale, il ransomware può essere molto impattante. Pensiamo al caso in cui una macchina dovesse essere attaccata durante le ore di picco; la produzione si arresterebbe e l'importo del riscatto potrebbe avere un impatto drastico dal punto di vista finanziario.

Il paradosso aziendale: la necessità della connettività cloud

Nel panorama competitivo di oggi, è praticamente impossibile pensare a macchinari senza connettività cloud. Essa consente di effettuare analisi dei dati in tempo reale, manutenzione predittiva e un'integrazione ottimale con altri sistemi. Il monitoraggio remoto delle prestazioni semplifica le operazioni e riduce il downtime delle macchine. Inoltre la manutenzione viene fatta quando serve, con un risparmio di tempo e risorse. Questa maggiore connettività richiede maggiore sicurezza. I rischi possono essere ridotti al minimo adottando le misure indicate in questo documento.



Fonte: IBM X-Force Threat Intelligence Index 2022

Presentazione di IXON

Il costruttore di macchine del futuro è un fornitore di servizi. Il punto di partenza è la connessione fisica con le macchine dei suoi clienti. Sia che si tratti dell'accesso remoto che per lo sviluppo di nuovi servizi basati sui dati delle macchine, senza questa connessione nulla è possibile. IXON, la piattaforma Industrial IoT progettata per i costruttori di macchine, offre il modo più sicuro e affidabile per mantenere la connessione con le macchine e i clienti in tutto il mondo.

Accesso remoto integrato

Molte soluzioni di accesso remoto sono strumenti stand alone, non connessi al resto della vostra strategia IoT e infrastruttura IT. A causa di questa interruzione, difficilmente i dati e le informazioni verranno scambiati agevolmente. IXON è l'unica piattaforma IoT con accesso remoto integrato: permette ai costruttori di gestire macchine e utenti in un'unica piattaforma, per l'accesso remoto e i servizi IoT. Per questo è una delle soluzioni più complete e avanzate sul mercato.

Piattaforma IoT completa

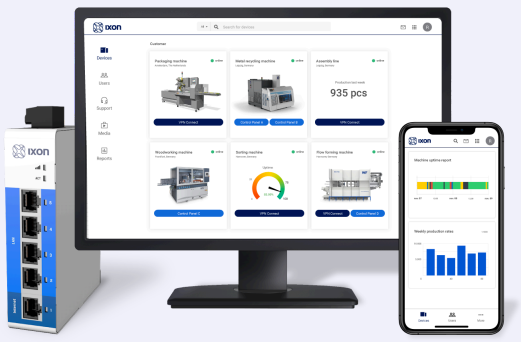
La vostra piattaforma IoT senza grandi investimenti iniziali e progetti di sviluppo software interminabili. IXON è una piattaforma Industrial IoT completa, low code e con molte funzionalità di default.

Piattaforma aperta ed espandibile

Dato che ciascun costruttore ha requisiti unici, la nostra piattaforma IIoT aperta ed espandibile offre infinite possibilità. Si integra con le vostre applicazioni IT esistenti tramite API e ti offre la possibilità di sviluppare applicazioni web personalizzate. Rendete la vostra strategia di servizi all'avanguardia con IXON.

Integrazione senza interruzioni dalla macchina al cloud

Gli edge gateway di IXON sono forniti con la piattaforma IXON Cloud. I gateway sono sviluppati da IXON e sono parte integrante dell'offerta. Per il massimo della sicurezza e dell'affidabilità della connessione dalla macchina al cloud, occorre un'integrazione perfetta tra hardware e software.



La nostra mission

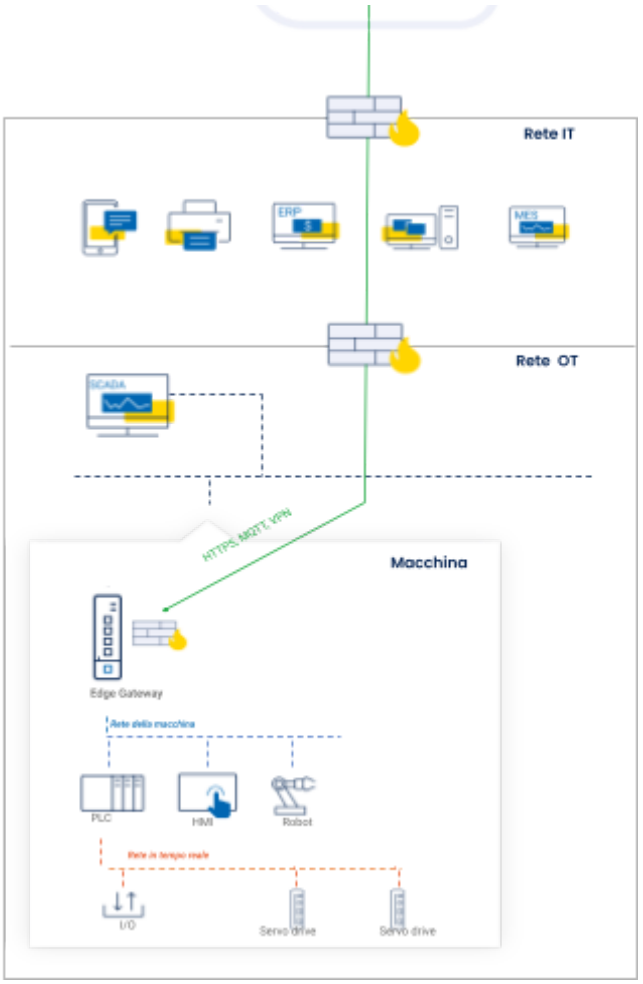
La nostra mission è quella di connettere i costruttori di macchine con i loro clienti. La stretta collaborazione tra end user e costruttori può migliorare i processi produttivi ed è alla base di un mondo più sostenibile in cui le macchine non si fermano mai.

Tutto sulla connessione macchina-cloud

La macchina si connette a IXON Cloud tramite l'edge gateway di IXON. Il gateway è montato su una guida DIN nel quadro elettrico della macchina.

Firewall

L'edge gateway è un firewall che separa la rete interna della macchina dalle reti OT e IT dello stabilimento produttivo. Questa separazione è fondamentale perché i componenti delle macchine non sono progettati per la sicurezza e spesso non sono aggiornati per aderire ai più recenti standard di sicurezza. Quindi il traffico tra i componenti della macchina, la rete IT dello stabilimento e internet deve essere ridotto al minimo.



Sistemi SCADA e MES

Se necessario, le impostazioni firewall dell'edge gateway possono consentire la comunicazione tra la macchina e i sistemi SCADA/MES.

Comunicazione in uscita

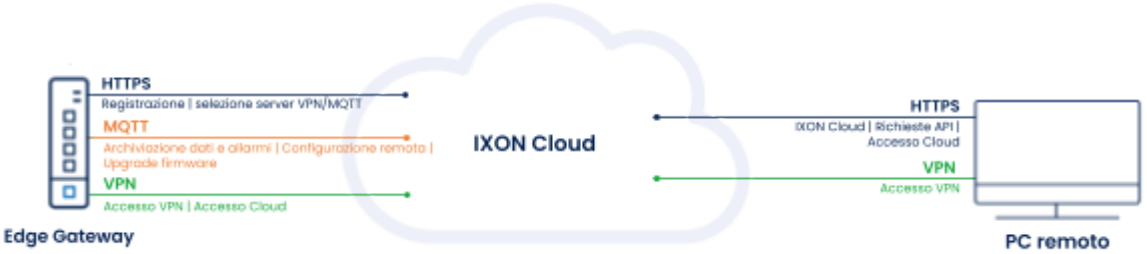
L'edge gateway comunica con la piattaforma IXON Cloud utilizzando solo connessioni in uscita. Ciò garantisce che tutte le connessioni in entrata (porte) nel firewall locale possano rimanere chiuse.

Il dispositivo ha 3 connessioni a IXON Cloud:

- Una connessione HTTPS per registrare il dispositivo e selezionare server VPN/MQTT.
- Una connessione MQTT per configurazione remota, aggiornamenti firmware e l'invio di avvisi e dati della macchina.
- Una connessione VPN per l'accesso remoto.

Tutto sulla piattaforma IXON Cloud

Crediamo che la trasparenza sia alla base della fiducia. Ecco perché vogliamo condividere informazioni sulla tecnologia alla base della piattaforma IXON Cloud. Questa sezione fornisce informazioni generali che potrebbero esserti utili per valutare la sicurezza di IXON. Informazioni più dettagliate disponibili su richiesta.



Servizi API
I servizi API sono il cuore di IXON Cloud e si trovano in data center ad Amsterdam. Gestiscono processi fondamentali tra cui l'autorizzazione, la configurazione di connessioni VPN e il recupero dei dati dai nostri database.

Servizi broker MQTT
I servizi broker MQTT di IXON vengono utilizzati per la distribuzione di configurazioni dei dispositivi, l'invio di comandi per l'upgrade dei firmware e per la trasmissione di log dei dati e notifiche. I servizi broker MQTT sono collocati in data center ad Amsterdam.

Server VPN
I server VPN di IXON si trovano in data center in tutto il mondo per fornire connessioni a bassa latenza. La rete di server VPN è ridondante, quindi se un server VPN non è disponibile, gli altri server lo sostituiscono automaticamente.

L'API decide quale server VPN è il più adatto per configurare un tunnel VPN sicuro, in base alla posizione fisica dell'edge gateway e al server VPN più vicino. Visita status.ixon.cloud per una panoramica dei server attuali.

Dall'altra parte del tunnel, il nostro client VPN è un'applicazione leggera che viene eseguita in background sul vostro computer. Questo permette al costruttore di configurare una connessione VPN sicura alla vostra macchina dal tuo browser.

Anche per i computer senza una connessione attiva dal client VPN, è comunque possibile accedere all'HMI o ai controlli web-based delle vostre macchine. Grazie a WebAccess, i dati delle macchine vengono inviati tramite l'edge gateway al

server VPN utilizzando la connessione VPN già stabilita e tali informazioni vengono poi inviate al vostro browser tramite HTTPS o una connessione WebSocket sicura.

Cluster Kubernetes

La piattaforma IXON Cloud contiene più cluster Kubernetes per l'attivazione e la gestione dei microservizi. Questo tipo di architettura garantisce scalabilità e disponibilità ottimali della piattaforma IXON Cloud. I microservizi consentono di strutturare le grandi applicazioni come una raccolta di applicazioni (servizi) più piccole e indipendenti, che possono essere gestite e aggiornate individualmente, senza interruzioni di servizio. Ogni microservizio è sviluppato come un Docker container.

Cluster database relazionali

Il database relazionale archivia informazioni su utenti, company e dispositivi nella piattaforma IXON Cloud. Il database è ridondato mediante una struttura Primario-Secondario tra più data center ad Amsterdam. Il Primario riceve ed elabora tutte le richieste di visualizzazione o modifica del database. Il Secondario replica tutti gli eventi di scrittura/aggiornamento sul Primario e crea un backup ogni quattro ore.

Cluster database di serie temporali

I dati delle macchine raccolti con data logging vengono inviati utilizzando il protocollo altamente efficiente MQTT.

L'edge gateway raccoglie i dati e li invia al nostro broker MQTT: un nodo centrale per la ricezione e l'invio di messaggi.
Poi viene applicato il timestamp e i dati vengono archiviati in un database buffer. Quindi, viene applicata una correzione del timestamp per tenere conto di eventuali discrepanze tra l'orologio interno dell'edge gateway e l'orario NTP (orario effettivo).

Infine, i dati vengono archiviati in un cluster di database di serie temporali, ospitato in un data center a Francoforte, in Germania. Il vantaggio principale del database di serie temporali è che è ottimizzato per la gestione dei dati con timestamp. Questo consente agli utenti di richiedere dati relativi a un lungo periodo di tempo in pochi millisecondi e di eseguire operazioni, come il calcolo del valore medio, in modo rapido ed estremamente efficiente. Inoltre, i database di serie temporali consentono opzioni avanzate di gestione del ciclo di vita dei dati, come l'aggregazione o il downsampling dei dati delle macchine.

Cluster database non relazionali

Il database non relazionale archivia i dati sugli eventi della piattaforma IXON Cloud, gli allarmi generati e gli eventi dell'audit trail. Questo database è configurato come set di repliche, in cui il server primario riceve ed elabora tutte le richieste, mentre il secondario replica il server primario per assicurare alta disponibilità e ridondanza. I server del database si trovano in diversi data center ad Amsterdam.

IXON e la sicurezza

In qualità di fornitore di prodotti di sicurezza informatica OT, IXON inizia prima di tutto mettendo in sicurezza la sua stessa organizzazione. La sicurezza informatica è integrata in tutte le procedure e i processi interni con un sistema completo di gestione della sicurezza delle informazioni (ISMS) e un sistema di gestione delle informazioni sulla privacy (PIMS).

Certificazioni e conformità

Il sistema ISMS di IXON è certificato in base allo **standard ISO 27001**, ovvero il punto di riferimento globale per la sicurezza delle informazioni nelle organizzazioni. Questa certificazione richiede la conformità a diversi requisiti, tra cui controllo degli accessi, sicurezza informatica, formazione e consapevolezza, conformità, gestione dei rischi e continuità operativa.

Inoltre, IXON è certificata ed è conforme ad altri standard. Di seguito una panoramica completa:

Certificazioni del sistema di gestione IXON:		
✓ ISO 9001	Qualità	Certificato
✓ ISO 27001	Sicurezza delle informazioni	Certificato
✓ ISO 27017	Sicurezza del cloud	Certificato
✓ ISO 27701	Privacy	Certificato

IXON è conforme a quanto segue:		
✓ IEC 62443-4-1	Sviluppo software sicuro	Certificato
✓ IEC 62443-4-2	Componente sicuro	Certificato

Perimetro di certificazione

I sistemi ISMS e PIMS comprendono tutte le attività aziendali di IXON, tra cui lo sviluppo di soluzioni di connettività cloud, la produzione di dispositivi gateway, la gestione e la manutenzione della piattaforma IXON Cloud e la gestione di informazioni che consentono l'identificazione personale.

Scegliendo un perimetro così ampio per la certificazione del nostro sistema ISMS, garantiamo la protezione dei dati in IXON Cloud e nei nostri sistemi interni.

Infrastruttura cloud

IXON Cloud è una rete avanzata di oltre 150 server distribuiti in tutto il mondo, ottimizzata per prestazioni di picco, disponibilità e sicurezza. Questi server sono ospitati da provider specializzati che aderiscono a rigorosi standard di sicurezza e sono certificati ISO 27001.

Tutti i server che gestiscono i dati si trovano nell'Unione europea e garantiscono la conformità alle normative del GDPR.

Di seguito riportiamo alcune misure fondamentali per mantenere la sicurezza dei server:

- Installazione automatica di aggiornamenti di sicurezza e blocco di traffico di rete non necessario.
- Monitoraggio server in tempo reale 24/7 con avvisi immediati di qualsiasi anomalia.
- Sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) che esamina l'output dei server per identificare eventuali attività sospette.
- Scansioni settimanali di vulnerabilità e test di penetrazione regolari eseguiti da terze parti sia sulla piattaforma IXON Cloud sia sugli edge gateway.

Soluzioni on-premise

IXON ha deciso deliberatamente di non fornire soluzioni server on-premise, a causa dei rischi associati. Queste soluzioni richiederebbero monitoraggio e manutenzioni continui e specialisti di sicurezza dedicati. Invece IXON si impegna a essere una piattaforma (SaaS) interamente gestita con misure di sicurezza solide (vedi *Misure tecniche e organizzative*).

Misure tecniche e organizzative

La sicurezza non riguarda solo la tecnologia, ma anche i processi e gli standard che seguiamo. In questo capitolo parleremo delle misure adottate da IXON, sia a livello tecnico sia organizzativo, per garantire che le tue apparecchiature rimangano al sicuro.

Sicurezza dell'infrastruttura

Rete dei server	IXON Cloud è una rete di 150 server, distribuiti globalmente tra diversi hosting provider. Tutti sono situati in data center che mantengono i più elevati standard di sicurezza.
Alta disponibilità	I server IXON sono configurati per un'alta disponibilità o hanno distribuzioni ridondanti, per garantire che un singolo guasto hardware o di rete non comprometta la disponibilità di IXON Cloud.
Backup	Viene effettuato il backup dei server stateful ogni settimana. Inoltre, vengono creati backup dei dati essenziali di clienti e macchine ogni 4 ore. Questi backup sono monitorati in tempo reale per verificarne l'accuratezza e vengono effettuati test di validità mensili.
Accesso ai server	Solo il personale IXON autorizzato, inclusi sviluppatori e amministratori, può accedere ai server. Questo è possibile grazie a chiavi SSH private e nomi utente unici. Tutte le attività legate ai server vengono registrate e controllate.
Monitoraggio in tempo reale	I server vengono monitorati costantemente con una serie di verifiche standard e personalizzate per analizzare le metriche interne. Eventuali deviazioni o anomalie vengono immediatamente segnalate al personale competente.
Configurazione dei server	Un nodo master gestisce la configurazione dei server, garantendo l'uniformità tra i server. Questo sistema consente anche la distribuzione semplice di nuovi server.
Hardening dei server	I nostri server sono sottoposti a un processo di hardening, per ridurre al minimo le vulnerabilità tramite l'eliminazione di protocolli inutilizzati, la restrizione delle autorizzazioni di accesso ai file e la richiesta di password efficaci.
Gestione patch	Le patch critiche vengono applicate entro un giorno. Ogni settimana, le patch software non critiche vengono valutate e quelle che migliorano l'uptime, le prestazioni o la sicurezza vengono distribuite.

Firewall	Ogni server contiene un firewall che adotta un approccio ”deny-all” e "permit-by-exception". Le eccezioni vengono valutate rigorosamente e devono essere il più severe possibile, adottando metodi come l'autorizzazione di protocolli o degli IP sorgente.
Scambio tra server	I server IXON Cloud operano in una rete mesh interna, per garantire che le comunicazioni tra i server non passino mai attraverso internet.

Confidenzialità e privacy dei dati

Privacy by design	Qualsiasi modifica alla gestione dei dati, dagli aggiornamenti software all’alternanza dei fornitori esterni o alle modifiche ai processi interni, deve superare l'analisi di impatto sulla privacy per garantire la privacy dei dati.
Conformità al GDPR	Le informazioni che consentono l'identificazione personale (PII) sono elaborate e archiviate da terze parti basate in UE in linea con la legislazione del GDPR, come indicato in "Elenco di terze parti". IXON ha nominato un privacy officer per garantire la conformità.
Proprietà dei dati	Tutti i dati personali e delle macchine archiviati o creati su IXON Cloud rimangono di vostra proprietà. IXON non può, in alcuna forma o misura, utilizzare in modo improprio, distribuire o vendere tali informazioni.
Conservazione dei dati	I dati restano disponibili finché l’account utente è attivo. Una volta eliminato l'account, i dati verranno rimossi dopo 3 mesi.
Codifica TLS	Le connessioni HTTPS e MQTT utilizzano il protocollo TLS 1.2 o superiore per la cifratura. Consentiamo solamente algoritmi di codifica solidi che supportano la perfect forward secrecy, utilizzando chiavi RSA da 4096 byte.
Crittografia VPN	Le connessioni VPN utilizzano certificati TLS monouso per l'autenticazione. Viene utilizzato AES-256-CBC per la cifratura e SHA512 per l'autenticazione.
Hash delle password	Le password IXON Cloud sono memorizzate come hash utilizzando Argon2id, configurato con 3 iterazioni, 4 livelli di parallelismo, 64 MiB di memoria e salt da 16 byte.

Gestione delle vulnerabilità

Scansione delle vulnerabilità	I server IXON Cloud vengono testati settimanalmente per le vulnerabilità utilizzando scansioni interne ed esterne.
Test di penetrazione	Ogni anno, la piattaforma IXON Cloud e gli edge gateway sono oggetto di almeno 2 test di penetrazione di terze parti. I test vanno dalle Black Box Evaluation dell'intero IXON Cloud alle White Box di modifiche significative all'architettura.
Analisi dei log	Tutti i log dei server vengono raccolti in un sistema di log centralizzato e analizzati automaticamente in base a regole di sicurezza secondo una community di esperti e personalizzate.

Gestione degli incidenti

Protocollo per violazioni di sicurezza	È in essere un protocollo per affrontare in modo efficace ed efficiente gli incidenti di sicurezza. In breve, il protocollo include i seguenti passaggi: 1) Verifica dell'incidente, 2) Contenimento, 3) Valutazione e 4) Conclusioni.
Notifica degli incidenti	Le parti e gli utenti interessati ricevono tempestivamente una notifica in caso di incidente di sicurezza (generalmente via e-mail). Cerchiamo di essere il più trasparenti possibile nelle nostre comunicazioni.
Formazione sugli incidenti	Ogni anno, utilizzando un ambiente simulato, replichiamo un'importante violazione di sicurezza per assicurarci che il personale IXON sia a conoscenza del proprio ruolo nel protocollo per violazioni di sicurezza.
Piano di continuità operativa	È in essere un piano per garantire che le operazioni aziendali continuino senza interruzioni durante eventi naturali o causati dall'uomo.

Sicurezza delle applicazioni

Autenticazione	L'accesso iniziale a IXON Cloud prevede la Basic Authentication. Dopo l'accesso, gli utenti ricevono un Bearer token valido per la durata della loro sessione.
Efficacia delle password	Richiediamo che le password siano considerate "impossibili da indovinare" (n. tentativi > 10^8) dal nostro strumento di stima della robustezza. Non costringiamo ad avere requisiti di complessità per le password. Il sistema blocca anche le password comunemente utilizzate.

Protezione da brute force	Ripetuti tentativi di accesso non riusciti (> 10 tentativi) portano a un blocco temporaneo. Il periodo aumenta con l'aumentare di tentativi falliti, fino a un massimo di 1 ora.
Autenticazione a più fattori	È possibile utilizzare le password monouso a tempo (TOTP) come fattore di autenticazione aggiuntivo. Possono essere attivate per utenti individuali o essere richieste per tutti gli utenti all'interno dell'ambiente IXON Cloud.
Autorizzazioni granulari	Gli amministratori possono perfezionare le autorizzazioni utilizzando ruoli e gruppi di utenti, modificando l'accesso a più utenti contemporaneamente. Queste autorizzazioni possono fornire accesso a tutti i dispositivi, occuparsi di dispositivi specifici (accesso LAN limitato) o limitare determinati servizi dei dispositivi, come VPN o WebAccess (WebVNC o WebHTTP).
Separazione logica dei dati	Sebbene i dati dei clienti si trovino in ambienti multi-tenant, implementiamo più livelli per proteggere la riservatezza dei dati. Inizialmente, le richieste convalidano il vostro Bearer token. Poi, viene effettuato il filtraggio dei dati in base a dominio, ID aziendale e ruolo di autorizzazione, restituendo solo le informazioni che si è autorizzati a visualizzare.
Controllo delle sessioni	Le sessioni IXON Cloud attive sono accessibili all'interno dei dettagli del vostro account. Implementare una modifica di sicurezza, come nel caso di aggiornamento della password, comporta la revoca automatica di tutte le sessioni attive.
Audit trail	IXON Cloud fornisce audit trail specifici per i dispositivi e relativi all'intera company, offrendo agli utenti un registro completo degli eventi passati.

Sviluppo software

Security by design	I requisiti di sicurezza sono definiti prima dello sviluppo e devono essere soddisfatti prima che sia possibile implementare le modifiche.
Peer review	Qualsiasi modifica al codice è sottoposta alla revisione di almeno uno sviluppatore senior imparziale. In questo modo garantiamo leggibilità, chiarezza e completezza. Tutti i problemi identificati devono essere risolti prima dell'approvazione.
Test automatici	Quando vengono apportate modifiche al sistema di versioning del software, il codice viene sottoposto a test automatici completi. Sono inclusi test unitari, scenario di test e valutazioni di sicurezza.

Staged deployment	Impieghiamo ambienti distinti per segregare codice (potenzialmente) non sicuro prima che arrivi alla produzione: • Sviluppo: viene eseguito localmente sui sistemi degli sviluppatori, per facilitare le modifiche del codice e test automatici. • Test: conserva le funzionalità completate e funge da piattaforma per test manuali. • Staging: contiene il codice pronto per la produzione e viene utilizzato per stress test e integrazione.

Sicurezza organizzativa

Revisione dei fornitori	I fornitori e terze parti sono oggetto di una revisione di sicurezza iniziale e successive verifiche annuali. I fornitori essenziali, come gli hosting provider, devono possedere un certificato ISO 27001 o equivalente.
Formazione e consapevolezza	Tutto il personale della sicurezza deve seguire una quota di formazione predefinita ogni trimestre. I nuovi assunti ricevono formazione sulle policy di sicurezza di IXON durante l'onboarding e tutto il personale effettua aggiornamenti regolari su argomenti di sicurezza pertinenti.
Policy management	Le nostre policy di sicurezza sono accessibili tramite pagina web interna. Le modifiche alle policy sono documentate e richiedono l'approvazione prima della pubblicazione. Le policy vengono sottoposte a revisione ogni due anni.
Gestione del rischio	Nel corso di valutazioni del rischio trimestrali vengono classificate le minacce in base a probabilità e impatto. I rischi che superano le soglie accettabili vengono documentati in un piano di intervento, in cui vengono delineate azioni correttive specifiche e le rispettive scadenze.
Protezione degli endpoint	Tutti gli hardware aziendali hanno una codifica del disco rigido e un software di protezione degli endpoint. Ogni settimana vengono eseguite scansioni approfondite antivirus e le anomalie vengono segnalate istantaneamente al nostro team di sicurezza.
Certificazioni	Certificazioni del sistema di gestione IXON: • ISO 9001: Gestione della qualità

	● ISO 27001: Gestione della sicurezza delle informazioni ● ISO 27017: Sicurezza delle informazioni del sistema cloud ● ISO 27701: Gestione della privacy L'ente notificato accreditato NCI effettua audit esterni ogni anno. IXON è inoltre conforme a quanto segue: ● IEC 62443-4-1: Sviluppo software sicuro ● IEC 62443-4-2: Componente sicuro
Audit interni	Ogni trimestre vengono effettuati audit interni da dipendenti IXON indipendenti.

Risorse aggiuntive

Condizioni d'uso di IXON	Include nel dettaglio tutte le clausole legali relative all'uso di IXON Cloud.
Informativa sulla privacy di IXON Cloud	Il documento spiega in termini semplici come gestiamo le vostre informazioni personali e come ci assicuriamo che restino al sicuro.
Status page di IXON	Mostra lo stato attuale della piattaforma IXON Cloud ed eventuali casi di inattività.
Avvisi di sicurezza di IXON	Questa directory contiene informazioni sugli incidenti di sicurezza passati, versioni e aggiornamenti di prodotti e servizi IXON.

Security Desk e Legal Desk
Offriamo documentazione completa, formazione e strumenti. Per i servizi digitali è fondamentale avere accordi su privacy dei dati, proprietà dei dati e responsabilità. IXON può aiutarti a capire gli accordi tra costruttori di macchine, proprietari di macchine e IXON. L'accesso ai Security Desk e Legal Desk di IXON è gratuito.

Per ulteriori informazioni, contatta il nostro Security Officer, Dylan Eikelenboom:

E-mail: security@ixon.cloud
Telefono: +31 (0)85 744 1105

Appendice A:

Raccomandazioni di implementazione

I prodotti IXON richiedono alcune scelte relative a impostazioni, funzionalità e connessioni, con un impatto diretto sui rischi di sicurezza. Le impostazioni predefinite degli edge gateway di IXON sono severe, ma compatibili al tempo stesso con la maggior parte dei macchinari. Tuttavia, a volte è necessario apportare modifiche. Questo capitolo indica i passaggi pratici per utilizzare in sicurezza il vostro ambiente IXON, garantendo la sicurezza delle vostre macchine.

I punti indicati sono da intendersi come best practice generali. Il singolo costruttore potrebbe avere evidenti motivi per comportarsi diversamente, ad esempio per policy aziendali, preferenze personali o casi d'uso particolari. È possibile farlo ovviamente, ma vanno considerati i potenziali rischi per la sicurezza.

Sicurezza di IXON Cloud

✔ Credenziali account efficaci
Quando create il vostro account, è fondamentale scegliere una password efficace che sia lunga, unica e difficile da indovinare. Attivate inoltre l'autenticazione a due fattori per aggiungere un ulteriore livello di sicurezza al tuo account richiedendo una seconda forma di verifica oltre alla password. Con questi due passaggi è praticamente impossibile che utenti non autorizzati accedano al vostro account.

✔ Gestione altri utenti
L'utente che crea la company su IXON Cloud avrà automaticamente i diritti di amministratore e potrà invitare altri utenti nella piattaforma. Valutate a chi inviare gli inviti. Di seguito un elenco di buone prassi generali:

- Invitate solo le persone che devono accedere a IXON Cloud.
- Avvisate preventivamente.
- Verificate e controllate gli indirizzi e-mail.
- Non invitate persone con account email condivisi (ad es. info@azienda.com).
- Fornite agli utenti solo le autorizzazioni di cui hanno bisogno (vedi sezione successiva).
- Aggiungete un messaggio che spieghi la necessità di password efficaci.
- Se un utente necessita solo di un accesso temporaneo, non dimenticate di impostare una data di scadenza.

Per far sì che tutti gli utenti della company utilizzino credenziali efficaci, consigliamo vivamente agli amministratori di attivare l'autenticazione a due fattori per tutti gli utenti.

✔ Principio del minimo privilegio

Fornite agli utenti solamente le autorizzazioni che servono unicamente per le loro attività. Inoltre, limitate l'accesso solo agli edge gateway di cui hanno bisogno. Come regola generale, è meglio creare un'eccezione e fornire a qualcuno autorizzazioni più elevate, anzichè fornire autorizzazioni di cui probabilmente non avranno mai bisogno.

Applicate regole particolarmente severe per le autorizzazioni di gestione utenti e gestione ruoli, poiché queste consentono di invitare altri utenti e impostare le autorizzazioni. Per semplicità d'utilizzo, create ruoli utente e gruppi utenti descrittivi per gestire gruppi di utenti in una volta.

✔ Aggiornamento tempestivo dei dipendenti in uscita

Quando una persona lascia l'azienda o cambia ruolo, valuta il prima possibile il suo accesso a IXON Cloud. Aggiornate le sue autorizzazioni di conseguenza o rimuovetele del tutto.

✔ Sessioni aperte solo su dispositivi attendibili

Durante l'accesso, potete scegliere l'opzione di mantenere l'accesso, che estende la sessione (il periodo durante il quale non ti verranno chieste le credenziali), da 24 ore a 30 giorni. Questo migliora la facilità d'utilizzo per i dispositivi protetti in cui voi siete gli unici utenti, ma costituisce un rischio in caso di dispositivi condivisi o presi in prestito. Analogamente, su questi dispositivi, non dimenticate di disconnettervi quando avete finito di utilizzare IXON Cloud. Dovreste controllare regolarmente le vostre sessioni attive e revocare quelle che non dovrebbero più esserlo.

✔ Controllo attività di IXON Cloud

Una revisione regolare dell'audit log può aiutarti a identificare eventuali attività insolite o sospette nella vostra company. L'audit log fornisce un registro di tutte le azioni effettuate nel vostro account, compresi accessi, modifiche alle autorizzazioni utente e molto altro. Inoltre, definite un momento in cui rivedere regolarmente tutti gli aspetti della sicurezza di IXON Cloud: utenti, autorizzazioni, sessioni, credenziali, ecc.

Sicurezza dei dispositivi

✔ Installazione nuovi dispositivi

I nuovi edge gateway devono essere installati in modo sicuro. In particolare, l'accesso fisico a dispositivi e PLC deve essere limitato effettuando l'installazione in un quadro elettrico o una stanza chiusa. Dopo tutto, l'accesso fisico all'edge gateway o alla macchina vi consente di connettervi direttamente alla macchina, aggirando il firewall.

Per registrare l'edge gateway a IXON Cloud si usa generalmente un file di configurazione (un file *ixrouter.conf*) su chiavetta USB. Dopo la registrazione, vi consigliamo di rimuovere l'USB dal dispositivo. Se inserita, l'edge gateway scrive le informazioni di log sull'USB per motivi di debugging e potrebbero esserci informazioni riservate. Vi consigliamo anche di eliminare il file *ixrouter.conf* dall'USB. In generale, non ci sono informazioni riservate nel file di configurazione, a meno che non si configuri l'edge gateway in modo che si connetta tramite connessione Wi-Fi autenticata. Comunque è possibile utilizzare il file di configurazione per registrare altri edge gateway al vostro ambiente IXON Cloud.

Infine, è importante modificare la password dell'interfaccia web dell'edge gateway. La password iniziale è unica per ogni dispositivo, ma è stampata sull'etichetta e potrebbe essere trovata da chiunque abbia accesso fisico. Una volta usata per l'accesso iniziale, cambiate la password usandone una lunga, unica e difficile da indovinare.

✔ Configurazione failover

Se possibile, configura i dispositivi in modo Multi-WAN, che fornisce funzionalità di failover in caso di interruzione della loro connessione internet principale.

✔ Attivazione controllo locale sull'accesso remoto

Connettete un interruttore al digital input dell'edge gateway per scegliere quando consentire le connessioni VPN. In questo modo, gli operatori hanno il controllo locale su accesso remoto e WebAccess.

✔ Implementazione patch

Consigliamo vivamente di aggiornare i dispositivi quando è disponibile una patch di sicurezza. È comunque buona prassi effettuare l'aggiornamento quando è disponibile una nuova versione. Sebbene non tutte le nuove versioni del firmware contengano patch di sicurezza, contengono comunque miglioramenti alla stabilità, nuove funzionalità e correzioni di bug. L'elenco delle modifiche e dei miglioramenti è disponibile su IXON Cloud o nelle nostre note di rilascio.

✔ Autorizzazione traffico necessario

Per consentire all'edge gateway di raggiungere la piattaforma IXON Cloud tramite internet, dovete autorizzare il traffico di rete in uscita valido nel firewall locale. Usate regole di firewall granulari per consentire solo il traffico necessario. La comunicazione dell'edge gateway ha le seguenti caratteristiche:

- l'edge gateway di IXON comunica con il protocollo TCP sulla porta in uscita 443*
- gli indirizzi IP indicati in whitelist.ixon.cloud sono destinazioni valide
- i domini IXON terminano con .ixon.net o .ayayot.com

** Il traffico potrebbe utilizzare la porta 8443 quando usa la modalità Stealth VPN o la porta 53 per le richieste DNS*

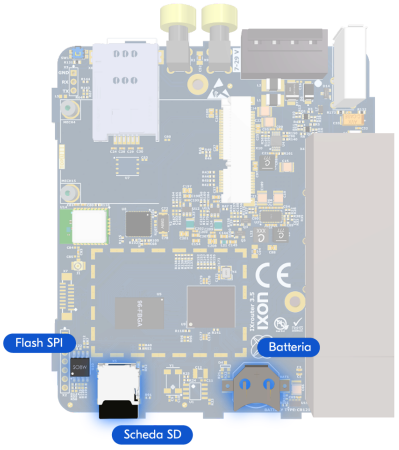
✔ Limitazione firewall

Per impostazione predefinita, il firewall dell'edge gateway è configurato nel modo più rigido possibile. Cambiate le regole del firewall solo se necessario, per evitare di consentire accessi indesiderati. Modifiche come il passaggio da LAN a WAN aumentano la probabilità di traffico doloso. Usate l'immagine qui sotto per determinare potenziali insidie:

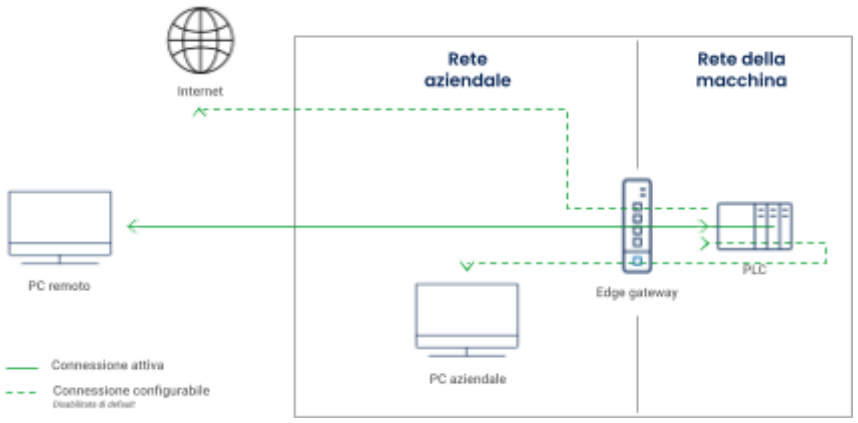
✔ Smaltimento dispositivi disattivati

Quando un dispositivo viene disinstallato e riutilizzato in ambiente diverso, consigliamo di ripristinare le impostazioni di fabbrica e rimuoverlo dalla piattaforma IXON Cloud per assicurarti che non rimangano dati precedenti. Dopo questa operazione, puoi utilizzarlo come un dispositivo nuovo.

Se un edge gateway viene disattivato, possono essere presenti dati riservati nel dispositivo. Il chip **Flash SPI** contiene chiavi di autenticazione utilizzate per identificarsi come edge gateway di IXON e la **scheda SD** potrebbe avere dati di logging delle macchine e core dump dopo un arresto anomalo. Aprite la scocca del dispositivo e rimuovete o distruggete queste parti.



Vi consigliamo anche di rimuovere la batteria a bottone e di smaltirla in modo rispettoso dell'ambiente.



Comunicazione

✔ Informazioni costanti su eventi di sicurezza, aggiornamenti e modifiche

Per essere sempre al corrente di tutto ciò che è direttamente e indirettamente collegato alla sicurezza, consultate le seguenti risorse:

- Stato IXON (status.ixon.cloud): mostra lo stato attuale della piattaforma IXON Cloud e potenziali inattività.
- Avvisi di sicurezza di IXON (support.ixon.cloud): contiene le informazioni più recenti su incidenti di sicurezza, versioni e aggiornamenti per tutti i prodotti e servizi IXON.
- Note di versione IXON (answers.ixon.cloud): indica tutti gli aggiornamenti software di piattaforma IXON Cloud, edge gateway o client VPN.

Appendice B:

Elenco di terze parti

IXON utilizza fornitori di piattaforme, fornitori di infrastrutture e altri partner commerciali di terze parti per fornire i suoi servizi ai clienti.

Cos'è un fornitore esterno?
Un fornitore esterno (o subcontractor) è una terza parte incaricata da IXON per eseguire parte dei suoi servizi e che potrebbe avere accesso all'infrastruttura di produzione con dati dei clienti o elaborare i dati dei clienti.
L'icona GDPR indica che la parte gestisce o potrebbe gestire le informazioni che potrebbero identificarti personalmente, in base a come utilizzi i nostri servizi.

Due diligence
IXON si occupa della due diligence per valutare la privacy dei dati e la postura di sicurezza informatica di (potenziali) subcontractor, sia prima dell'incarico che annualmente. Le nostre attività sono pensate per garantire che l'elaborazione venga effettuata solamente da entità con capacità idonee a soddisfare i nostri standard di protezione dei dati.

Informazioni di contatto
Se avete altre domande sull'impiego di fornitori da parte di IXON o hai dubbi, contattaci all'indirizzo privacy@ixon.cloud.

Infrastruttura di IXON Cloud

IXON Cloud è composto da circa 150 server basati su Linux che si trovano principalmente nell'UE. I server sono forniti da hosting provider, su cui viene installato il software proprietario di IXON. Ciascun provider utilizzato per ospitare i server di IXON Cloud possiede la certificazione ISO 27001 e la conformità al GDPR come requisiti minimi.

Database

Azienda	Posizione/i dei server	Tipo di dati archiviati
Aiven aiven.io	Germania	Dati delle macchine (quando previsto dal piano tariffario)
GDPR Digital Ocean LLC digitalocean.com	Paesi Bassi	Dati di audit trail
		Dati dei clienti
		Dati delle macchine (backup)
InfluxData influxdata.com	Germania	Dati delle macchine
GDPR UpCloud Ltd. upcloud.com	Paesi Bassi	Dati di audit trail
		Dati dei clienti

Server VPN

Nota: i dati trasmessi tramite VPN sono codificati e leggibili solo dal destinatario previsto (ovvero il client). Il traffico VPN non è archiviato in alcun modo.

Azienda	Posizione/i dei server
Digital Ocean LLC digitalocean.com	Singapore, Paesi Bassi e Stati Uniti
Exoscale exoscale.com	Austria e Germania
Alibaba Cloud alibabacloud.com	Cina
Linode LLC linode.com	Stati Uniti
UpCloud Ltd. upcloud.com	Germania e Paesi Bassi
Vultr Holdings Corp. vultr.com	Australia, Germania e Stati Uniti

Infrastrutture ausiliarie

Azienda	Posizione/i dei server	Finalità
Upcloud upcloud.com	Paesi Bassi	Reti interne, CDN e monitoraggio server
Digital Ocean LLC digitalocean.com	Paesi Bassi	API, reti interne, bilanciamento carico, monitoraggio server, broker MQTT
	Singapore e Stati Uniti	API (interna)
Vultr Holdings Corp. vultr.com	Paesi Bassi	Hosting di dominio e monitoraggio server
TransIP transip.eu	Paesi Bassi	Monitoraggio server e provisioning automatico dei server

Piattaforma IXON Cloud

Azienda	Finalità	Posizione dei server
Akamai akamai.com	Servizi CDN	
Apple apple.com	App store	
ClouDNS cloudns.net	Servizi DNS	
Firebase firebase.google.com	Messaggi pushover	
Google LLC play.google.com	App store	
GDPR ElasticCloud elastic.co/cloud	Logging centralizzato	Paesi Bassi
GDPR Mailchimp mailchimp.com	Servizi e-mail	Stati Uniti
Realtime Register realtimeregister.com	Servizi DNS	
Segment segment.com	Identificazione utenti	
Sentry sentry.io	Tracciamento errori	
Tenable tenable.com	Scansione vulnerabilità di sicurezza	
GDPR TransIP www.transip.eu	Backup dei dati dei clienti	Paesi Bassi
Userpilot userpilot.com	Onboarding utenti	

Servizi ausiliari

Azienda	Finalità	Posizione/i dei server
Discourse discourse.org	Forum pubblico (answers.ixon.cloud)	
GitLab about.gitlab.com	Versioning del software	
Google LLC datastudio.google.com	Analisi aziendale	
GDPR Hubspot hubspot.com	Sito web aziendale (www.ixon.cloud) e integrazione con CRM	Germania
Microsoft Corp. powerbi.microsoft.com	Analisi aziendale	
Readme readme.com	Pagina di supporto (developer.ixon.cloud)	
GDPR Salesforce.com Inc. salesforce.com	CRM	Francia e Germania
Status.io status.io	Pagina di stato (status.ixon.cloud)	
Zendesk zendesk.com	Pagina di supporto (support.ixon.cloud)	

Conclusioni

IXON fornisce una piattaforma Industrial IoT sicura in grado di migliorare la collaborazione tra i costruttori di macchine e i produttori, per raggiungere prestazioni ottimali. Grazie a server globali ridondanti e a controlli di sicurezza completi, offriamo una soluzione semplice e affidabile che ti offre la tranquillità che cerchi.

La fiducia che ripongono in noi più di 2.500 aziende in tutto il mondo, con oltre 70.000 macchine connesse, non si ottiene facilmente. Queste aziende hanno scelto IXON perché sanno che investire nella nostra tecnologia porta crescita e vantaggi misurabili. Attraverso l'innovazione continua, aiutiamo i nostri utenti a massimizzare i propri investimenti.

IXON si assume con orgoglio la responsabilità di proteggere i vostri asset più preziosi. La sicurezza non è solo una promessa, è nel DNA di tutto ciò che facciamo.

La scelta fidata dei costruttori di macchine in tutto il mondo

Headquarter di IXON
Beugen, Paesi Bassi
Tel.: +31 85 744 1105

www.ixon.cloud

support@ixon.cloud
sales@ixon.cloud
security@ixon.cloud