Gestione dei problemi della sicurezza informatica nelle piattaforme di monitoraggio remoto dei Data Center

White paper 239

Revisione 0

di Torben Karup Nielsen e Patrick Donovan

Sintesi

I servizi di monitoraggio remoto digitale provvedono al monitoraggio in tempo reale e all'analisi dei dati dei sistemi dell'infrastruttura fisica dei Data Center. Queste moderne piattaforme basate sul cloud sono estremamente promettenti in termini di riduzione delle interruzioni, dei tempi medi di ripristino e del sovraccarico operativo, incrementando l'efficienza energetica degli impianti di alimentazione e di raffreddamento. Si stima che i costi per far fronte a violazioni della sicurezza informatica quadruplicheranno nei prossimi anni (raggiungendo 2 trilioni di dollari entro il 2019[1]), tuttavia, questi sistemi potrebbero costituire potenzialmente un punto di attacco per i criminali informatici. Questo whitepaper descrive i principali aspetti di sicurezza correlati allo sviluppo e all'uso di piattaforme di monitoraggio remoto digitale basate sul cloud, per la riservatezza dei dati e per la protezione dei sistemi infrastrutturali. Conoscere i sistemi per sviluppare e implementare correttamente queste piattaforme è estremamente utile per valutare la qualità dei fornitori di servizi di monitoraggio remoto e delle loro soluzioni.

Introduzione

Le tecnologie informatiche mission-critical dipendono esclusivamente dai sistemi dell'infrastruttura fisica sottostante. Questi sistemi sono fondamentali per il funzionamento delle risorse informatiche ma rappresentando notevoli spese di capitale e di esercizio. Questa criticità e i relativi costi richiedono il monitoraggio e la gestione di tali risorse. I software DCIM (Data Center Infrastructure Management) per la gestione dell'infrastruttura del Data Center e i servizi di monitoraggio remoto possono contribuire a incrementare l'efficienza e l'affidabilità delle risorse informatiche con notifiche preventive e una vista centralizzata di tutte le risorse, del loro stato e delle relative interdipendenze.

I servizi di monitoraggio remoto (cioè il monitoraggio effettuato da terzi esterni alla rete) sono diffusi da vari anni. Tradizionalmente, questi servizi implicano aggiornamenti intermittenti dello stato tramite l'invio di email dai sistemi infrastrutturali a quelli deputati al monitoraggio. Questi servizi si sono evoluti in servizi digitali (online) basati sul cloud in cui il monitoraggio viene effettuato in tempo reale con l'uso di servizi informatici (ad es. archiviazione su cloud, analisi dati e app mobili). Il white paper 237, ***La trasformazione della gestione e della manutenzione dei Data Center tramite il monitoraggio remoto digitale***, descrive ulteriormente questo moderno tipo di monitoraggio remoto. Queste piattaforme di monitoraggio digitale sono estremamente promettenti in termini di riduzione delle interruzioni, dei tempi medi di ripristino e del sovraccarico operativo, incrementando l'efficienza energetica degli impianti di alimentazione e di raffreddamento. I motori di analisi dei dati garantiscono informazioni approfondite che sarebbe impossibile ottenere con i tradizionali sistemi di monitoraggio offline. Tali informazioni approfondite consentono di identificare importanti tendenze e condizioni per ridurre i costi ed evitare le interruzioni.

Le piattaforme di monitoraggio remoto digitale operano tramite il collegamento dei sistemi dell'infrastruttura del Data Center che inviano un flusso continuo di dati a un gateway che le inoltra all'esterno della rete o nel cloud. Questi dati, quindi, vengono monitorati e analizzati da persone e motori di analisi dei dati. Alla fine, avviene un ciclo di feedback dei sistemi e del team di monitoraggio con gli operatori del Data Center. Gli operatori del Data Center accedono ai dashboard di monitoraggio all'interno della rete tramite il gateway o al cloud della piattaforma esternamente alla rete tramite un'app mobile o un computer in un NOC remoto. La **Figura 1** illustra un'architettura di base di una moderna piattaforma di monitoraggio digitale.

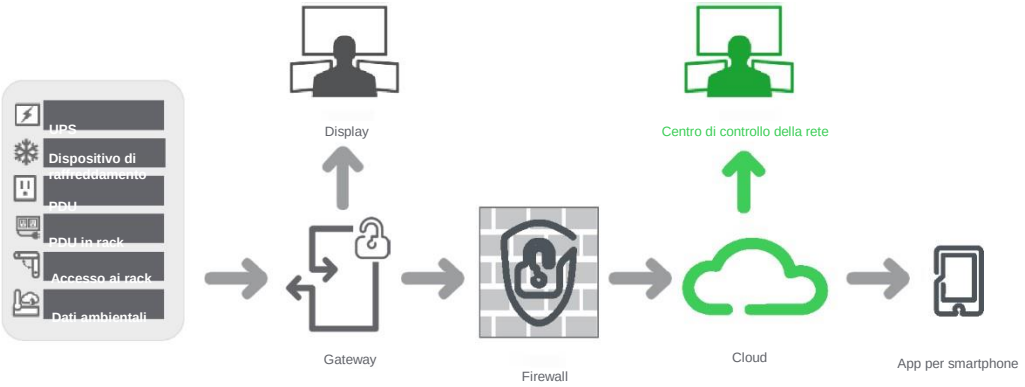

Figura 1
Architettura di monitoraggio digitale consigliata

Si stima che i costi dovuti a violazioni della sicurezza informatica quadruplicheranno nei prossimi anni (raggiungendo 2 trilioni di dollari entro il 2019[1]), tuttavia, queste piattaforme di monitoraggio collegate esternamente potrebbero costituire un percorso di attacco per i criminali informatici. Attualmente, le minacce della sicurezza informatica sono sempre presenti e la natura degli attacchi è in costante evoluzione.

[1] http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#45018db93bb0

La prevenzione di questi attacchi per evitare furti, perdite di dati e interruzioni del sistema richiede una piattaforma di monitoraggio e una vigilanza costante effettuata da un team DevOps dedicato. Prima della scelta e dell'implementazione di una piattaforma di monitoraggio digitale, è opportuno valutare le soluzioni offerte dai fornitori non solo in base alle caratteristiche e alle funzioni, ma anche in base alla capacità di proteggere i dati e il sistema da attacchi informatici. Per conoscere il livello di sicurezza in una piattaforma occorre sapere come viene sviluppata, implementata e gestita. Tali conoscenze saranno utili per valutare i meriti dei fornitori di servizi di monitoraggio remoto e per garantire una maggiore protezione del sistema e dei dati dopo l'implementazione. Questo white paper fornisce una panoramica sul processo che garantisce un ciclo di vita di sviluppo sicuro (SDL), descrivendo le modalità di progettazione e sviluppo di un prodotto. Vengono illustrate, inoltre, alcune caratteristiche e funzioni essenziali delle piattaforme di monitoraggio remoto digitale per ridurre il rischio di attacchi informatici. Anche se questa discussione è incentrata sulla piattaforma del fornitore, occorre tenere presente che anche la sicurezza del Data Center e/o della rete informatica richiedono particolare attenzione.

Ciclo SDL (Secure Development Lifecycle)

Il ciclo SDL è un processo con cui si valuta la sicurezza in tutto il ciclo di vita dello sviluppo di prodotti e soluzioni. Originariamente è stato sviluppato e proposto da Microsoft[2]. L'uso di un processo SDL per la gestione dello sviluppo, dell'implementazione e della gestione di una piattaforma di monitoraggio indica che il fornitore attua misure adeguate per garantire la sicurezza e la conformità alle norme.
Il fornitore dovrebbe utilizzare un processo conforme allo standard ISO 27034[3].

Figura 2
Principali procedure di un processo SDL (Secure Development Lifecycle) per la gestione di tutto il processo di sviluppo del software

Creazione di un modello di minacce

Per la fondazione OWASP (Open Web Application Security Project) la creazione di un modello di minacce è "una metodologia di analisi della sicurezza di un'applicazione". È un approccio strutturato che consente l'identificazione, la quantificazione e la gestione dei rischi di sicurezza associati a un'applicazione. La creazione di un modello di minacce non è un approccio alla revisione del codice, ma un processo complementare a quello di revisione del codice di sicurezza. L'inclusione della creazione di un modello di minacce nel ciclo SDL contribuisce a garantire che l'applicazione è stata sviluppata integrando la sicurezza sin dall'inizio. Tutto ciò, assieme alla documentazione prodotta nell'ambito del processo di creazione di un modello di minacce, può fornire al revisore una maggiore comprensione del sistema e la possibilità di riconoscere i punti di ingresso dell'applicazione e le relative minacce associate. Il concetto di creazione di un modello di minacce non è nuovo, ma negli ultimi anni ha subito notevoli modifiche metodologiche. Attualmente, la creazione di modelli di minacce controlla il sistema dal punto di vista dei potenziali malintenzionati e non dal punto di vista di chi deve difendersi da tali malintenzionati. "

Questo white paper identifica 8 procedure fondamentali, illustrate nella **Figura 2**. Ognuna viene descritta brevemente di seguito. Le sezioni successive di questo white paper evidenziano i principali aspetti specifici di queste procedure, in relazione allo sviluppo e alla gestione di una piattaforma di monitoraggio remoto digitale del Data Center basata sul cloud.

Formazione

I dipendenti dovrebbero essere sottoposti a un programma di formazione continuo per la progettazione, lo sviluppo, i test e l'implementazione di soluzioni più sicure.

Requisiti

Le funzioni di sicurezza informatica e i requisiti di sicurezza da includere nello sviluppo del prodotto dovrebbero essere enumerati in maniera chiara e dettagliata.

Progettazione

Vengono prodotti documenti relativi all'architettura di sicurezza conformi agli standard progettuali accettati nel settore, per lo sviluppo delle funzioni di sicurezza richieste dal cliente. Questi documenti sono sottoposti a revisione e vengono creati modelli di minacce (v. **trafiletto laterale**[4]) per identificare, quantificare e gestire i potenziali rischi per la sicurezza.

Sviluppo

L'implementazione del progetto architetturale della sicurezza nel prodotto segue una fase di progettazione dettagliata ed è guidata dalla documentazione di procedure ottimali e standard di codifica. Allo sviluppo partecipano vari strumenti di sicurezza, ad esempio analisi statica, binaria e dinamica del codice da utilizzare.

[2] https://en.wikipedia.org/wiki/Microsoft_Security_Development_Lifecycle
[3] http://www.iso27001security.com/html/27034.html
[4] https://www.owasp.org/index.php/Application_Threat_Modeling

Verifica

I test di sicurezza sull'implementazione del prodotto vengono condotti da una prospettiva del modello di minacce e della garanzia di solidità. Nell'ambito dei test sono inclusi i requisiti normativi e la strategia di sviluppo.

Rilascio

Documentazione sulla sicurezza che definisce le modalità con cui incrementare il livello di sicurezza nell'installazione, nella messa in servizio, nella manutenzione, nella gestione e dismissione del prodotto. Gli artefatti di sicurezza[5] vengono revisionati sulla base dei requisiti originari e del livello di sicurezza desiderato o specificato.

Implementazione

Il team di sviluppo del prodotto o il responsabile dello sviluppo dovrebbe essere disponibile a fornire addestramento e consigli ai tecnici dell'assistenza in relazione alle procedure più corrette per l'installazione e l'ottimizzazione delle funzioni di sicurezza. I team di assistenza dovrebbero essere in grado di fornire assistenza ai clienti durante l'installazione, la gestione e l'aggiornamento di prodotti e soluzioni per tutto il loro ciclo di vita.

Risposta

Dovrebbe essere creato un team di risposta alle emergenze informatiche che gestisca le vulnerabilità e fornisca assistenza ai clienti in caso di incidenti. Questo team dovrebbe essere costituito dallo stesso gruppo di persone che hanno sviluppato l'applicazione. Ciò implica che tutti dovrebbero conoscere dettagliatamente il prodotto.

Aspetti chiave dello sviluppo e della distribuzione di una piattaforma sicura

Questa sezione descrive con maggiore dettaglio alcuni aspetti chiave delle procedure SDL critiche per garantire la sicurezza informatica delle piattaforme di monitoraggio remoto digitale. La consapevolezza del livello di idoneità di una piattaforma impone un confronto con il fornitore.

Le persone

Una fonte o un veicolo di attacco informatico è riconducibile a qualcuno all'interno dell'organizzazione o della rete. Tale persona non deve essere necessariamente un malintenzionato. Anche un dipendente fedele e corretto può diventare inconsapevolmente un veicolo di attacco. Siccome i dati dell'infrastruttura vengono inviati tramite una piattaforma di monitoraggio remoto digitale, è importante conoscere le modalità con cui il fornitore gestisce il proprio personale, sia chi sviluppa la piattaforma sia chi la implementa e la gestisce. La **Tabella 1** elenca gli elementi fondamentali da valutare in relazione alla modalità con cui il fornitore gestisce i propri dipendenti.

[5] Gli artefatti di sicurezza rappresentano gli esiti documentali dei test effettuati nella fase di verifica. A questo punto del processo, quindi, si valuta se l'applicazione sviluppata è conforme ai livello di sicurezza originariamente richiesto.

Tabella 1
Condizioni e azioni da valutare in relazione alla modalità con cui il fornitore gestisce i propri dipendenti

Gestione dei dipendenti da parte del fornitore

Assunzione	• Tutti i potenziali dipendenti sono sottoposti a una verifica del curriculum • Gli operatori della piattaforma dovrebbero essere esperti nella gestione delle infrastrutture di Data Center • Gli sviluppatori sono esperti nelle procedure SDL
Formazione e gestione	• Formazione indispensabile sulla sicurezza informatica basata sul ruolo (sviluppatore, operatore, tecnico di assistenza sul campo, dipendente generico) • Monitoraggio e documentazione del completamento del corso di formazione e relativi punteggi • Programma di formazione continuo per i necessari aggiornamenti • Processo di escalation per la gestione delle violazioni delle politiche di sicurezza
Accesso alla rete e alle risorse informatiche	• Principio del privilegio minimo: agli utenti viene concesso l'accesso solo alle risorse e alle funzioni informatiche e di rete strettamente necessarie per lo svolgimento del loro lavoro • Tutti gli utenti sono dotati di account singolarmente identificabili, che garantiscono controllo e affidabilità totali dell'accesso, dell'uso e delle modifiche del sistema.

Progettazione di un'architettura sicura

La piattaforma di monitoraggio remoto digitale dovrebbe essere progettata assegnando la priorità alla sicurezza informatica. Di seguito sono indicati alcuni attributi e standard ottimali consigliati per una piattaforma di monitoraggio digitale:

Attributi e standard ottimali consigliati per la piattaforma

Solo connessioni in uscita	Il gateway che acquisisce i dati dei clienti nella rete dovrebbe essere l'unico a gestire connessioni verso l'esterno: dal gateway al servizio cloud. Nessuno all'esterno del gateway dovrebbe essere in grado di collegarsi. Il polling del gateway può essere effettuato solo con una connessione sicura creata dal gateway. Siccome il gateway non consente connessioni in entrata, esso non può essere un veicolo di attacco.
HTTPS	La piattaforma dovrebbe utilizzare solo un protocollo HTTPS (Hyper Text Transfer Protocol) sicuro per proteggere i dati riservati e l'integrità dei dati in transito.
Autenticazione a più fattori	L'autenticazione deve avvenire tramite più fattori, vale a dire una combinazione di nome utente e password e un codice temporaneo inviato tramite un messaggio di testo a un telefono verificato come secondo fattore, per ridurre il rischio di furto di credenziali per l'accesso al sistema. Questa misura di accesso alla piattaforma dovrebbe essere applicata anche al fornitore, in modo che se la rete interna del fornitore subisce un attacco, il malintenzionato non possa accedere ai dati della piattaforma di monitoraggio remoto o al codice sorgente.
Crittografia dei dati	I dati sensibili dovrebbero essere crittografati mentre sono "a riposo" (cioè archiviati su disco o nel cloud) e mentre sono "in transito" (cioè durante la trasmissione dal gateway al servizio cloud). Tutte le credenziali utente, i dati di fatturazione e le informazioni sugli ordini, sia a riposo che in transito, dovrebbero essere crittografati.
Codice sorgente sicuro	Il codice sorgente della piattaforma dovrebbe adempiere ai requisiti delle norme di conformità del codice sorgente, ad es. NIST SP 800-53 Rev. 4 e DISA STIG 3.9. Al momento in cui viene scritto questo white paper, queste norme sono appoggiate dal governo degli Stati Uniti. La conformità viene verificata tramite l'analisi statica del codice[6]. Tutte le modifiche del codice dovrebbero essere revisionate da colleghi prima dell'accettazione. Questo processo garantisce che il codice non possa subire modifiche senza che almeno due sviluppatori le accettino. L'implementazione e la configurazione delle modifiche del codice sorgente avvengono tramite l'automazione e script predefiniti, per ridurre il rischio di errori umani.

[6] https://en.wikipedia.org/wiki/Static_program_analysis

Test di sicurezza

I test di sicurezza sono fondamentali nello sviluppo di una piattaforma di monitoraggio digitale e rappresentano l'unico mezzo con cui è possibile valutare adeguatamente la sicurezza dell'architettura e del progetto prima dell'implementazione. I test hanno inizio durante la fase di sviluppo. La **Tabella 2** riepiloga le procedure di test consigliate.

Tabella 2
Test di sicurezza per lo sviluppo di una piattaforma

Procedure di test consigliate	
Analisi statica del codice	L'analisi statica del codice implica l'identificazione dei punti deboli del codice sorgente prima del build e dell'implementazione. Tutto il codice dovrebbe essere esaminato prima di ogni build, per eliminare eventuali problemi prima dello sviluppo dell'applicazione.
Test di penetrazione	I test di penetrazione rappresentano un metodo per scoprire eventuali vulnerabilità tramite test della piattaforma e della rete che potrebbero essere effettuati da un malintenzionato. I test possono essere effettuati da un punto di vista di un malintenzionato esterno (Black Box) o interno (White Box). I team di test dovrebbero essere distinti e indipendenti dal team di sviluppo, e dovrebbero essere specializzati nei test di penetrazione. A volte, i fornitori di test sono esterni all'azienda.
Scansioni di sicurezza continue	La piattaforma dovrebbe essere sottoposta a scansioni e test continui (dopo l'implementazione) per identificare nuove vulnerabilità. Tali operazioni dovrebbero essere effettuate con strumenti di scansione in grado di individuare vulnerabilità della sicurezza note.

Il ruolo dei team "DevOps"

La vigilanza continua dopo l'implementazione è particolarmente importante, forse anche di più dello sviluppo di un prodotto sicuro con cui cominciare. La sicurezza informatica è un bersaglio mobile sottoposto a un numero e a un tipo di minacce in continua evoluzione. Oltre alla modalità di progettazione e sviluppo della piattaforma, anche la sicurezza dipende dalla capacità del fornitore di scoprire, reagire e rimediare tempestivamente in caso di problemi di sicurezza.

Un team DevOps[7] dedicato (v. **trafiletto laterale**) dovrebbe essere istituito dal fornitore responsabile della sicurezza della piattaforma e della risposta alle minacce dopo l'implementazione della soluzione. Le funzioni basilari di questo team sono tre:

- **Rilevamento**: il team dovrebbe effettuare scansioni di sicurezza continue (come sopra descritto) tramite strumenti di rilevamento aggiornati di fornitori attendibili. Oltre a ciò, tutti i registri di tutti i componenti del sistema dovrebbero essere acquisiti e revisionati continuamente per individuare eventuali anomalie.
- **Reazione**: il team DevOps dovrebbe offrire una copertura "24/7" e dovrebbe essere in grado di segnalare automaticamente eventuali problemi critici della piattaforma o del gateway.
- **Rimedio**: tramite la formazione, il monitoraggio, le prove e i test automatici delle funzionalità e della sicurezza, i team DevOps dovrebbero essere in grado di risolvere con sicurezza i problemi in tutti gli ambienti.

Per il team DevOps, i parametri fondamentali sono due: Tempo medio di rilevamento e tempo medio di ripristino, vale a dire che il team è concentrato sul rilevamento dei problemi e sul conseguente ripristino (problemi di sicurezza o squisitamente tecnici) nella maniera più rapida ed efficiente possibile. Si tenga presente che questo approccio è diverso da quello più tradizionale, incentrato sul tempo medio tra due guasti, un parametro di minore utilità per una piattaforma cloud in quanto non attiene alla rapidità con cui vengono risolti i problemi. Per i team DevOps, due elementi di interesse influiscono su questi parametri: sicurezza della rete e sicurezza fisica. Le procedure consigliate sono descritte brevemente.

"DevOps"

Questo termine è una contrazione dei termini "development" (sviluppo) e "operations" (implementazione). La definizione di Wikipedia (v. nota a piè di pagina) è più o meno la seguente: una metodologia di sviluppo del software che punta alla comunicazione, collaborazione e integrazione tra sviluppatori e addetti all'implementazione delle tecnologie informatiche, con l'automazione del processo di fornitura del software e di modifica dell'infrastruttura.
È finalizzata alla creazione di una cultura e di un ambiente in cui le build, i test e il rilascio del software avvengano in maniera rapida, frequente e più affidabile. In relazione alle piattaforme di monitoraggio remoto digitale, il team dovrebbe essere costituito da addetti allo sviluppo e all'implementazione della piattaforma.

[7] https://en.wikipedia.org/wiki/DevOps

Sicurezza della rete

I team DevOps devono monitorare costantemente la sicurezza della rete della piattaforma del fornitore, che deve essere isolata il più possibile dal mondo esterno per garantire la sicurezza e la riservatezza dei dati. A tal fine, un metodo efficace consiste nell'uso di jump server o host. Un jump server è un computer consolidato e monitorato che generalmente include un firewall locale che funge da controllo accessi tra reti con protocollo di sicurezza di livello diverso. Questi host sono configurati con SSH (secure shell), un protocollo di rete crittografico che protegge i dati della rete dall'intercettazione. L'uso di certificati SSL (secure socket layer) garantisce che i dashboard e le pagine Web della piattaforma siano utilizzati dai reali possessori (cioè il fornitore, il proprietario o il provider). Questi certificati avviano il protocollo Internet HTTPS sicuro (sopra descritto) utilizzando la porta 443 del router. Tutto ciò garantisce una connessione sicura tra la piattaforma o il browser o l'app mobile dell'utente. Dovrebbero essere utilizzati anche elenchi di controllo accessi (ACL) residenti sul jump server per garantirne la disponibilità solo a chi dovrebbe accedere. In realtà, tutti i server che compongono la piattaforma cloud del servizio dovrebbero essere protetti tramite ACL (access control list).
Per un potenziale hacker sarà più difficile utilizzare un server violato come piattaforma per attaccarne altri, dal momento che i server sono tra loro invisibili.

Sicurezza fisica

Un elemento importante – ma spesso ignorato – della responsabilità del team nel rilevamento di *tutte* le minacce è il monitoraggio dell'infrastruttura *fisica*. Generalmente, si ritiene che la sicurezza fisica riguardi solo gli addetti alla sicurezza fisica dell'infrastruttura del fornitore che gestiscono e monitorano l'accesso all'edificio. Alcuni aspetti della sicurezza fisica, tuttavia, richiedono la gestione o almeno la cooperazione con il team DevOps e informatico. Questi aspetti includono l'accesso delle persone al Data Center, alle sale e armadi informatici e alle aree di sviluppo del software. Anche il dipartimento informatico e i team DevOps dovrebbero contribuire a impedire agli estranei l'accesso ai computer. A tal fine, tutti gli sviluppatori e gli operatori devono:

- Proteggere i computer portatili con la crittografia del disco
- Utilizzare un firewall locale
- Utilizzare password "sicure"
- Attivare il blocco dello schermo dopo un breve conto alla rovescia

Il team DevOps del fornitore, inoltre, dovrebbe garantire l'esecuzione di test di penetrazione regolari e non programmati, per controllare la sicurezza fisica e la sicurezza della rete nelle sedi di sviluppo e implementazione della piattaforma cloud. Per garantire risultati imparziali, infine, questi test dovrebbero essere effettuati da aziende terze.

Conclusioni

Le moderne piattaforme di monitoraggio digitale possono ridurre notevolmente le interruzioni, i tempi medi di ripristino e i sovraccarichi operativi, incrementando l'efficienza energetica degli impianti di alimentazione e di raffreddamento. I motori di analisi dei dati possono produrre informazioni utili e approfondite sulle principali tendenze. I sistemi di monitoraggio online, tuttavia, potrebbero rappresentare potenziali canali di attacco. Attuando adeguate procedure di sviluppo, implementazione e gestione, tuttavia, queste piattaforme basate sul cloud possono rivelarsi molto sicure. È importante discutere approfonditamente con i fornitori del monitoraggio per comprendere il loro livello di implementazione e conformità a tali procedure. Queste informazioni contribuiranno all'assunzione di decisioni efficaci nella scelta del fornitore e alla tranquillità dopo l'implementazione.

Informazioni sugli autori

Torben Karup Nielsen è Program Manager in Schneider Electric. Vanta un'esperienza quasi decennale nello sviluppo di software, incluse varie versioni delle premiate suite software DCIM di Schneider Electric. Nel corso della sua collaborazione con Schneider Electric, Torben ha fornito un prezioso contribuito con la stesura di vari white paper ed è titolare di svariati brevetti correlati alle soluzioni software per la gestione dei Data Center. Prima del suo ingresso in Schneider Electric, Torben si è occupato di teorie informatiche.

Patrick Donovan è Senior Research Analyst per il Data Center Science Center di Schneider Electric. Vanta un'esperienza ultraventennale sviluppo e nel supporto di sistemi di alimentazione e raffreddamento critici per il settore informatico di Schneider Electric; ha realizzato, inoltre, diverse soluzioni per la disponibilità, l'efficienza e la protezione dell'alimentazione. Autore di molti white paper, articoli di settore e valutazioni tecnologiche, le sue ricerche sulle tecnologie e sul mercato delle infrastrutture fisiche per Data Center rappresentano un guida preziosa sui migliori standard in materia di pianificazione, progettazione e gestione dei Data Center.

Risorse

La trasformazione della gestione e della manutenzione dei Data Center tramite il monitoraggio remoto digitale
White paper 233

Sfoglia tutti i white paper
whitepapers.apc.com

Sfoglia tutti i TradeOff Tools™
tools.apc.com

Contatti

Per formulare pareri e commenti sul contenuto di questo white paper:

Data Center Science Center
DCSC@Schneider-Electric.com

Per formulare richieste specifiche sulla progettazione dei Data Center:

Rivolgersi al rappresentante Schneider Electric all'indirizzo
www.apc.com/support/contact/index.cfm

© 2016 Schneider Electric. Tutti i diritti riservati.