www.thenextfactory.it

The NEXT Factory

DBInformation
digital, business & publishing

3 | INDUSTRIA 4.0 | TECNOLOGIE INNOVATIVE | AUTOMAZIONE

ECONOMIA IL DECRETO RILANCIO
EVENTI SPS DIGITAL DAYS
IOT DOVE SIAMO
IN COPERTINA L'ADDITIVE

Anno 4° - Giugno/Luglio 2020 - n°3

Proteggersi con il cloud

CLOUDPROTECT È IL PROGETTO PORTATO AVANTI DA WIBU-SYSTEMS E IMPORTANTI PARTNER UNIVERSITARI PER COSTRUIRE UN SISTEMA CLOUD SCALABILE, SICURO E PERFORMANTE PER LA PROTEZIONE DEL SOFTWARE E LA GESTIONE DELLE LICENZE.

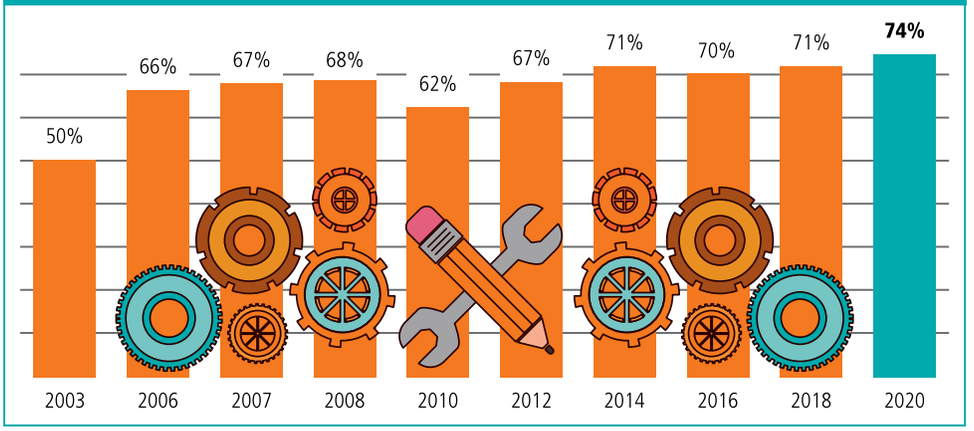
di Daniela Previtali

La protezione di software, beni digitali e proprietà intellettuale è diventata sempre più complessa negli anni e ancora di più con la crescente automazione nel settore industriale. Nel suo ultimo rapporto sulla pirateria di prodotto, l'associazione tedesca VDMA, che raggruppa i locali produttori attivi nel campo dell'industria meccanica e dell'impiantistica, evidenzia che il fenomeno, legato alla pirateria di prodotti e marchi, ha raggiunto il massimo storico attestandosi al 74% delle aziende, con danni economici stimati pari a 7,6 miliardi di euro l'anno. Per le aziende con più di 500 dipendenti, il tasso è ancora più alto: circa il 90%. Oltre alla perdita di fatturato e di posti di lavoro, le aziende interessate subiscono anche conseguenze difficilmente quantificabili in termini monetari come danno di immagine, perdita del vantaggio competitivo o richieste legali ingiustificate. Il know how coinvolto potrebbe essere rappresentato tanto dall'algoritmo altamente confidenziale di una macchina deputata al taglio laser, dai dati di configurazione di una saldatrice o da un blueprint per una stampante 3D. Gli approcci tradizionali alla protezione del software (nei suoi aspetti di salvaguardia

A sinistra: CloudProtect è un progetto di ricerca e sviluppo finanziato dal governo tedesco che vede coinvolti il Politecnico di Darmstadt, l'Università di Scienze Applicate di Offenburg e Wibu-Systems (uno dei tre principali vendor al mondo nella gestione sicura delle licenze software)

A destra: nel suo ultimo rapporto sulla pirateria di prodotto, l'associazione tedesca VDMA, che raggruppa i locali produttori attivi nel campo dell'industria meccanica e dell'impiantistica, fa emergere una tendenza preoccupante

Andamento annuale delle aziende colpite da pirateria di prodotto e di marchio nei settori dell'ingegneria meccanica e della costruzione di impianti



di riservatezza e integrità) combinano crittografia, offuscamento del codice ed elementi sicuri hardware o software locali, in qualità di anchors of trust. Sono questi ultimi a fornire il substrato necessario a crittografare e decrittare il codice dell'applicazione e i dati sensibili durante il runtime di un sistema.

Allo stesso tempo, l'accesso alle funzionalità protette del software può essere impiegato per implementare modelli commerciali di licenza, cioè di accesso a una parte specifica del software nel rispetto delle policy di sicurezza e delle politiche commerciali. Tuttavia, questo metodo non è necessariamente funzionale (tecnicamente ed economicamente) quando si fa riferimento a sistemi fisicamente e logicamente distribuiti su larga scala. La questione diventa pertanto se sia possibile fornire le stesse funzionalità tipiche di una chiave di protezione (in gergo, dongle) sottoforma di servizi cloud. Questo lo scopo di un progetto di ricerca e sviluppo, finanziato dal governo tedesco, che prende il nome di CloudProtect e che vede il Politecnico di Darmstadt, l'Università di Scienze Applicate di Offenburg e Wibu-Systems (uno dei tre principali vendor al mondo nella gestione sicura delle licenze software) impegnati per tre anni nella costruzione di un servizio cloud altamente scalabile, sicuro e performante.

I REQUISITI TECNICI DI UNA SOLUZIONE CLOUD

Le attuali soluzioni on premise di protezione e gestione licenze software lasciano ancora diverse questioni irrisolte:

- le dongles sono a prova di manomissione ma, se perse, lo sono anche le chiavi di decrittazione in esse archiviate;
- le dongles di tipo software (e relative chiavi di decrittazione) sono notevolmente più facili da attaccare, specialmente quando una macchina viene utilizzata in un ambiente non affidabile;
- se un produttore di software vuole offrire una soluzione interamente su cloud eventualmente in combinazione con una macchina, il servizio di protezione e gestione licenze dovrebbe essere offerto anche come servizio (SaaS - Software as a Service);
- le attuali soluzioni on premise, che utilizzano un server locale per la gestione delle licenze di grandi gruppi di utenti o macchine, non possono essere impiegate direttamente in un ambiente cloud;
- gli attuali sistemi di gestione licenze on premise si basano su parametri molto grossolani, mentre sarebbe auspicabile misurare con precisione come viene utilizzato un software (in conformità con le norme vigenti sulla privacy).

Si rende pertanto necessario implementare i seguenti requisiti tecnici:

- il servizio di gestione licenze su cloud deve fornire il materiale crittografico richiesto per consentire al consumatore del servizio di decodificare il software in fase di runtime;
- il consumatore deve potere interagire in tempo reale con tale servizio e, se in possesso di licenza commerciale valida, ricevere le chiavi digitali atte a eseguire la decrittazione;
- il proprietario del software deve potere definire a quali intervalli sia necessario verificare la presenza della licenza;
- se una connessione di rete non è di-

È POSSIBILE FORNIRE LE FUNZIONALITÀ DI UNA CHIAVE DI PROTEZIONE SOTTOFORMA DI SERVIZI CLOUD?

sponibile per un tempo configurabile, l'utilizzo del software deve essere comunque garantito;
- il server licenze su cloud deve essere in grado di gestire in parallelo molteplici richieste di convalida delle licenze a un ritmo elevato;
- i dati scambiati devono essere protetti a livello di trasferimento e di messaggistica.

I REQUISITI COMMERCIALI

Il costo complessivo di tale servizio (costi tecnici e amministrativi puri) dovrà essere inferiore ai ricavi generati. Sebbene questo requisito suoni banale, il calcolo dovrà tenere conto del fatto che il materiale crittografico non consiste più di un elemento locale e prevedere invece consumi in termini di elettricità e connettività. Bisognerà anche considerare che, in un modello cloud, le verifiche delle licenze devono potere essere eseguite per migliaia di utenti finali o di servizi e che i cicli di CPU richiesti devono essere pagati dall'operatore del cloud. Questo impone di ridurre al minimo i costi, volendo rendere la soluzione per la gestione licenze su cloud concorrenziale rispetto a una soluzione tradizionale on premise.

COSA PROPONE IL MERCATO OGGI

La maggior parte delle soluzioni disponibili non attua una vera e propria protezione del software, ma piuttosto un controllo accessi basato su una licenza acquistata.

Al contrario, Wibu-Systems ha già lanciato lo scorso anno CodeMeter Cloud, una nuova tecnologia pienamente interoperabile con i propri metodi tradizionali basati su contenitori licenze software e hardware. Gli sviluppatori di software possono continuare a utilizzare CodeMeter Protection Suite, un insieme di moduli dedicati alla protezione di specifici linguaggi e pensati tanto per i sistemi nativi, Java, .NET, quanto embedded e PLC. L'aspetto innovativo risiede nel fatto che le licenze e le chiavi crittografiche utilizzate per verificarne la validità sono ora archiviate in un'applicazione web.

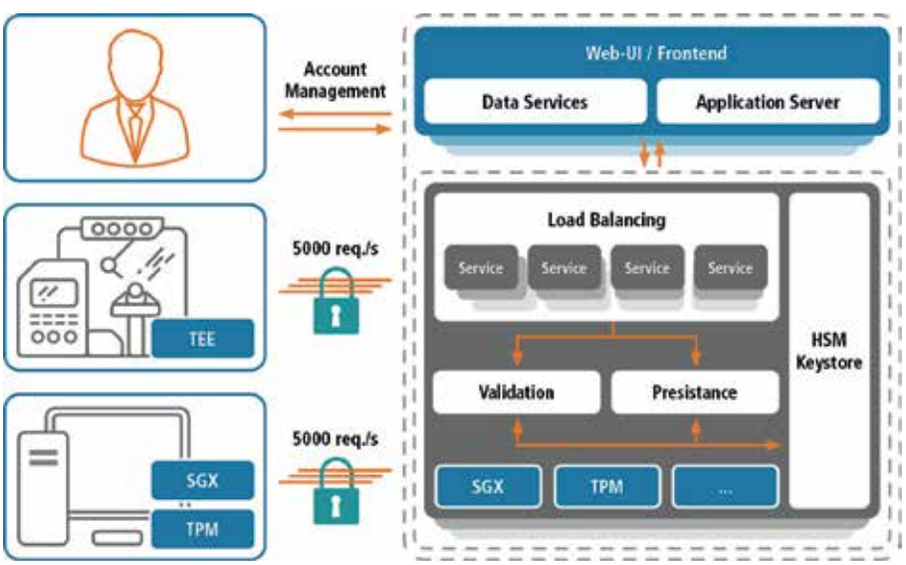
Ciò comporta che la licenza rimanga sempre nel cloud per tutta la sua validità e che gli utenti ricevano solo le proprie credenziali, create e gestite dall'ISV (Independent Software Vendor) attraverso CodeMeter Cloud Manager. Mediante tali credenziali, gli utenti hanno accesso a un CmCloudContainer, un contenitore licenze sul cloud di Wibu-Systems.

Qualsiasi richiesta di accesso al software protetto con CodeMeter Protection Suite è mediata dalla runtime (CodeMeter Runtime) che accompagna il software stesso. La frequenza e il livello di tali richieste possono essere configurati in modo granulare con CodeMeter Cloud.

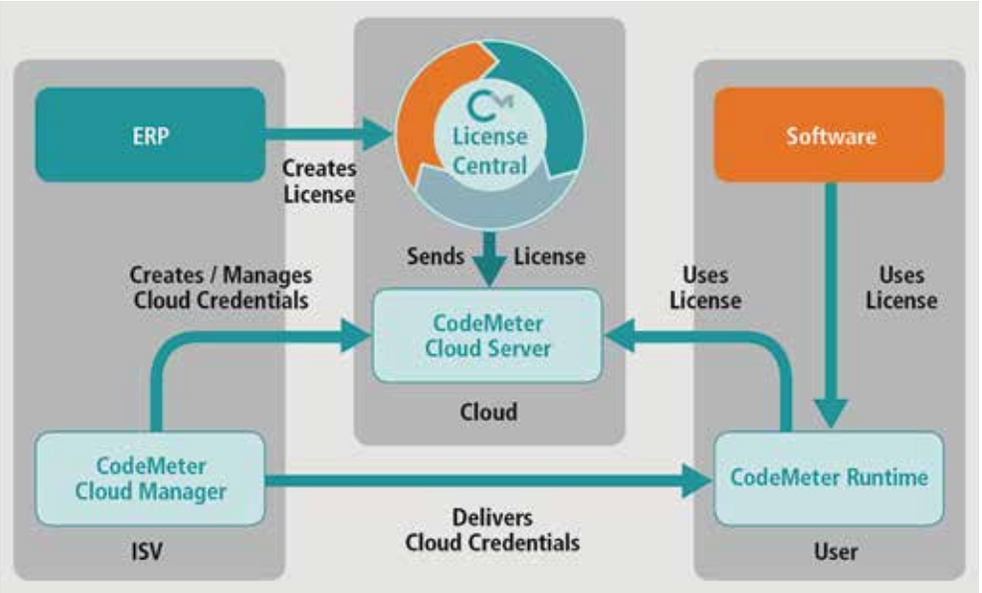
Nel caso di una licenza mancante o se non fosse consentito l'accesso a una funzione specifica, l'applicazione protetta semplicemente non funzionerebbe e all'utente verrebbe mostrato un messaggio di errore. CodeMeter Cloud è stato progettato dando la massima priorità all'aspetto delle prestazioni. L'architettura web include un livello in memoria che interagisce con un database NoSQL.

Insieme forniscono, in un ambiente estremamente sicuro, prestazioni elevate anche nel caso di molteplici interrogazioni di licenza simultanee. Un'istanza di CodeMeter Cloud Server è costituita da tre livelli distinti: bilanciamento del carico, livello servizi per la gestione delle licenze, la generazione e la relativa distribuzione delle chiavi crittografiche e la persistenza responsabile della memorizzazione dei dati su CodeMeter Cloud Server. Uno dei vantaggi principali di CodeMeter Cloud sta nel fatto che, al contrario delle soluzioni di gestione licenze tradizionali le quali comportano

LE ATTUALI SOLUZIONI ON PREMISE DI PROTEZIONE LICENZE SOFTWARE LASCIANO DIVERSE QUESTIONI IRRISOLTE



Nello schema, una sintesi del progetto CloudProtect



Il workflow di CodeMeter Cloud

CODEMETER CLOUD È STATO PROGETTATO DANDO LA MASSIMA PRIORITÀ ALL'ASPETTO PRESTAZIONALE

un ruolo attivo per gli utenti nel caso di restituzione delle licenze quando queste debbano essere utilizzate su un altro dispositivo, con CodeMeter Cloud l'utente può rivalersi della licenza da un altro dispositivo senza alcuna azione specifica da parte sua, purché si tratti del medesimo utente con le stesse credenziali.

IL PROGETTO CLOUDPROTECT

Con il progetto collaborativo CloudProtect, l'obiettivo è spingersi oltre. Un'istanza di CloudProtect mostra un bilanciatore di carico ad alta disponibilità (per esempio, basato su NGINX) per distribuire le richieste di convalida delle licenze che vengono ricevute in contemporanea. Il progetto prende in carico una richiesta ogni 10-15 s per utente finale. Un server cloud medio dovrebbe servire 20 ISV, ciascuno con 5.000 clienti attivi. In media, si prevede che un tale server debba potere gestire circa 10.000 richieste in parallelo al secondo. Come utente finale si intendono anche una macchina o un servizio collegato a un dispositivo IoT.

Un client che esegue un software protetto richiede un demon proprietario. Al momento, si tratta di un programma separato (.dll), che media le richieste al cloud. In futuro, questa funzionalità dovrebbe essere compilata direttamente nel codice protetto.

Questo demon avvierà anche una cifratura punto-a-punto tra gli host, nonché un canale cifrato end-to-end tra i servizi, sulla base di un'implementazione proprietaria allineata ai concetti principali della specifica TLS 1.3 (Transport Layer Security) attualmente emergente.

Un'archiviazione delle chiavi su HSM (Hardware Security Module) supporterà la gestione sicura delle chiavi root crittografiche.

Le richieste di licenza saranno distribuite in un cluster di strutture dati in-memory (per esempio, REDIS) e la persistenza finale avverrà in un cluster NoSQL (per esempio, basato su MongoDB). Questa funzionalità di base sarà offerta come macchina virtuale su server, con un minimo di 256 GB RAM, poiché l'accesso veloce alla memoria è un requisito tecnico essenziale. Una gerarchia di chiavi generata a partire da una chiave root controllata da Wibu-Systems sarà responsabile della concessione di chiavi agli ISV per il rilascio delle loro licenze. Questa gerarchia di chiavi verrà utilizzata anche per abilitare l'autenticazione di un client al cloud.

Per funzionalità come la gestione delle identità degli utenti e degli account, verrà poi offerto un set di servizi REST, in combinazione con i tradizionali web frameworks full-stack (per esempio Angular o Vaadin), che opereranno sulla base di servizi cloud out-of-the-box come Amazon RDS in associazione, per esempio, ai server applicativi scalabili Amazon Beanstalk.

Nell'ambito del progetto CloudProtect, si studierà come utilizzare le tecnologie di trust esistenti nell'ambito della protezione del software. Come elemento sicuro lato cliente, si valuterà la comprovata funzionalità TPM (Trusted Platform Module), per esempio, per proteggere ulteriori chiavi di cifratura locali o per generare numeri casuali.

Ci rivolgeremo in particolare ai clienti IoT che utilizzano un hardware minimo, come un Raspberry Pi 3 provvisto del chip Optiga™ TPM di Infineon. E da ultimo, sia lato client che lato server, si valuteranno le tecnologie Intel SGX (Software Guard Extensions) e TEE (Trusted Execution Environment) per supportare l'esecuzione isolata delle funzioni. ■

Daniela Previtali è Global Marketing Director di Wibu-Systems AG