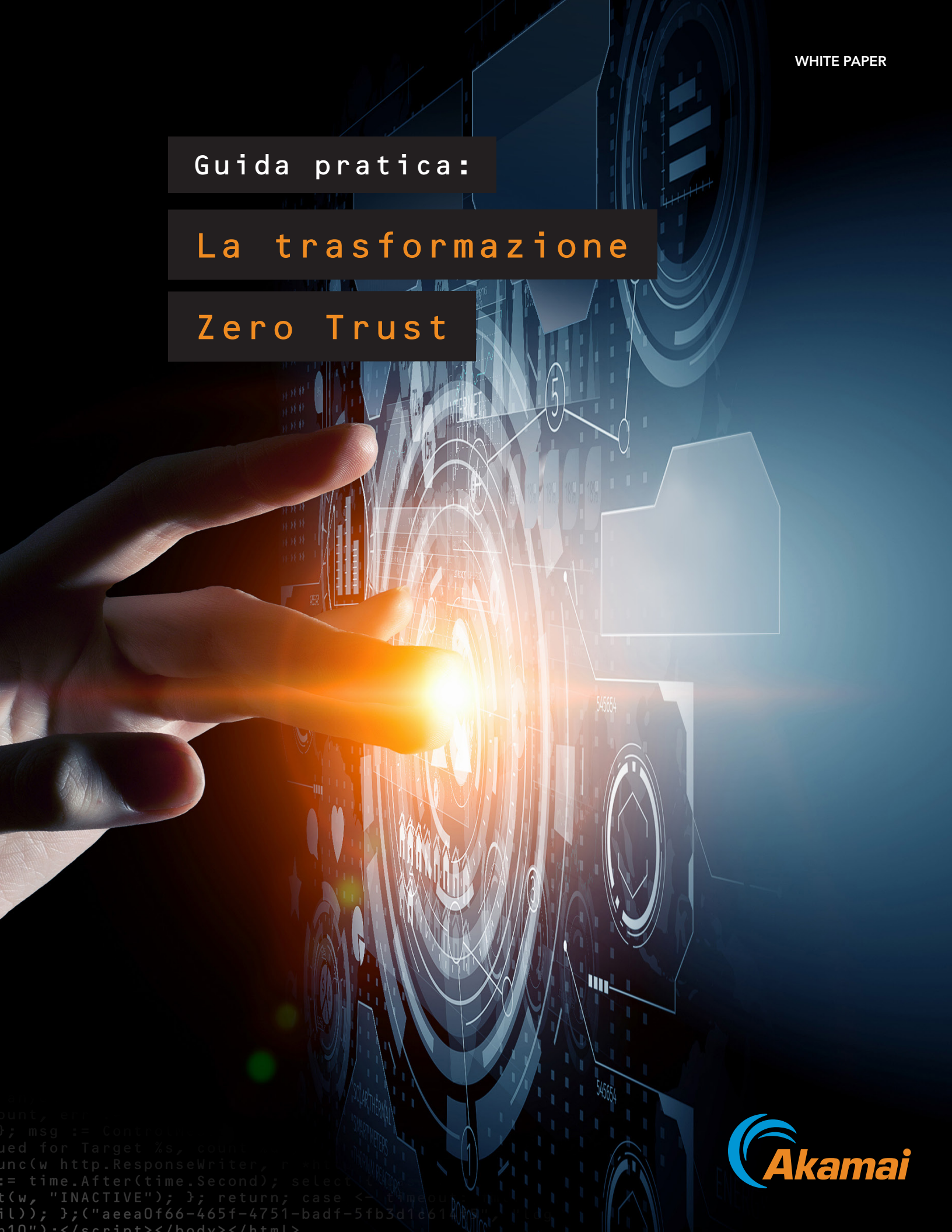
WHITE PAPER

Guida pratica:

La trasformazione Zero Trust



Akamai

Analisi riassuntiva

Nell'odierno panorama aziendale, non ci si può basare su un concetto di perimetro di rete, che considera tutti gli utenti che si trovano al di fuori della zona di controllo dell'azienda come malintenzionati e, viceversa, coloro che si trovano al suo interno come onesti e ben intenzionati. L'ampia adozione delle applicazioni SaaS, la migrazione ad architetture basate sul cloud, un crescente numero di utenti remoti e un afflusso di dispositivi BYOD hanno reso irrilevante la sicurezza basata sul perimetro. Inoltre, una difesa concentrata sul perimetro richiede la gestione delle appliance e delle policy di sicurezza, nonché frequenti aggiornamenti software, il che aumenta la complessità operativa e grava ulteriormente sui team IT già sovraccarichi di lavoro. Mentre la superficie soggetta agli attacchi si espande e le limitate risorse IT faticano a controllare un'architettura di rete sempre più complicata, i cybercriminali diventano sempre più abili, sofisticati e incoraggiati a eludere le misure di sicurezza. È necessario un sistema di sicurezza strategico in grado di affrontare queste specifiche sfide.

Cos'è il modello di sicurezza Zero Trust e perché è importante?

Un modello Zero Trust sostituisce un'architettura di sicurezza incentrata sul perimetro, garantendo che le decisioni relative alla sicurezza e all'accesso vengano applicate dinamicamente in base alle identità, ai dispositivi e al contesto dell'utente. Un sistema di sicurezza Zero Trust prevede, inoltre, che solo gli utenti e i dispositivi autenticati e autorizzati possano accedere alle applicazioni e ai dati, proteggendo, al contempo, applicazioni e utenti da avanzate minacce su Internet.

Per avanzare nel percorso verso l'adozione del modello Zero Trust, proteggendo, al contempo, utenti e applicazioni (nonché il futuro delle vostre attività aziendali), vi consigliamo di iniziare a:

Fornire agli utenti l'accesso solo alle applicazioni necessarie, non all'intera rete

Le tecnologie di accesso remoto legacy, come la VPN (Virtual Private Network), non sono in grado di soddisfare le crescenti richieste delle odierne aziende digitali prive di perimetri. La VPN tradizionale crea una minaccia per la sicurezza aziendale perché apre intrinsecamente una falla nel firewall, fornendo un accesso alla rete senza restrizioni. Una volta penetrato nella rete, l'autore di un attacco è libero di muoversi lateralmente per accedere e sfruttare qualsiasi sistema o applicazione che si trova al suo interno. Le VPN tradizionali non solo espongono l'azienda a rischi di sicurezza, ma sono anche soluzioni complesse che richiedono significative risorse IT per la gestione di hardware e software, oltre a risultare costose da mantenere e gestire.

La segmentazione della rete, a volte considerata una contromisura all'accesso indiscriminato, si è dimostrata costosa, difficile da implementare e complessa da gestire. Infine, non riduce il rischio poiché l'accesso "illimitato" consente comunque un movimento laterale all'interno della rete. Pur suddividendo in comparti il traffico laterale all'interno di una sottorete, questa strategia non è in grado di arrestare la diffusione orizzontale all'interno della stessa sottorete.

Per proteggere la vostra azienda e adottare il modello Zero Trust, è consigliabile concedere agli utenti l'accesso solo alle applicazioni di cui necessitano per il loro ruolo. Inoltre, conviene basare questo accesso sui diritti e sull'identità degli utenti, sul comportamento dei dispositivi, sull'autenticazione e sull'autorizzazione. Queste best practice ridurranno gli attacchi laterali, limitando l'esposizione alla rete. L'eliminazione delle VPN tradizionali migliorerà la user experience, aumenterà la produttività della forza lavoro e ridurrà le richieste all'helpdesk. Inoltre, evitare di affidarsi ancora ad una combinazione di firewall, hardware e software implica una riduzione dei costi di manutenzione per l'IT. Le autorizzazioni in base alle applicazioni migliorano anche la governance, fornendo visibilità e informazioni sulle persone che accedono alle applicazioni, sulla direzione dei dati e sulle modalità di accesso.

Concedete agli utenti solo l'accesso alle applicazioni di cui necessitano, basandolo sui diritti e sull'identità degli utenti, sul comportamento dei dispositivi, sull'autenticazione e sull'autorizzazione.

Isolare l'infrastruttura di rete dall'Internet pubblico

L'esposizione delle applicazioni interne e dell'infrastruttura di accesso a Internet le rende vulnerabili agli attacchi DDoS, SQL injection e ad altri attacchi a livello di applicazioni. I cybercriminali stanno diventando sempre più astuti: utilizzano tecniche in continua evoluzione per analizzare le configurazioni di rete aziendali al fine di individuare applicazioni vulnerabili e dati preziosi. Pertanto, le aziende devono isolare l'architettura delle applicazioni e degli accessi dall'Internet pubblico per evitare che venga presa di mira da malintenzionati che utilizzano porte in ascolto aperte.
Se i cybercriminali non riescono a trovare la rete o a stabilire quali applicazioni e servizi sono in esecuzione sul dispositivo preso di mira, non possono attaccarlo.

Abilitare la soluzione WAF per proteggere le applicazioni aziendali

I moderni attacchi informatici sono ipermirati: i malintenzionati sfruttano il social engineering (e-mail, social media, messaggistica istantanea, SMS, ecc.) per colpire i singoli utenti attirandoli con modalità altamente pertinenti e personalizzate. I cybercriminali cercano specifici utenti con superiorità di grado, competenze e livelli di accesso appropriati, quindi lanciano gli attacchi alle applicazioni mirati alle autorizzazioni di tali utenti.

Se il dispositivo di un utente viene compromesso, viene spesso utilizzato come dispositivo zombie per sferrare, a insaputa del proprietario, attacchi alle applicazioni aziendali considerate protette dal firewall. Anche se la maggior parte delle organizzazioni utilizza una soluzione WAF (Web Application Firewall) per proteggere da tali attacchi le proprie applicazioni destinate a utenti esterni, molte aziende non hanno esteso questa protezione alle applicazioni aziendali all'interno della rete. Una soluzione WAF può proteggere le applicazioni interne e i dati sottostanti da attacchi a livello di applicazioni e attacchi injection, come SQL injection, MFE (Malicious File Execution), CSRF (Cross-Site Request Forgery) e Cross-Site Scripting.

I cybercriminali prenderanno di mira un dispositivo, lo trasformeranno in un dispositivo zombie e lo utilizzeranno per attaccare le applicazioni ritenute sicure e protette da un firewall.

Applicare la verifica delle identità, l'autenticazione e l'autorizzazione prima di fornire l'accesso

I sistemi digitali concedono l'accesso a chiunque inserisca la password corretta, senza verificare l'identità della persona. L'utilizzo di credenziali semplici e password ripetute aumenta significativamente i rischi e la superficie soggetta agli attacchi di un'azienda. Nel panorama delle minacce odierne, non è più sufficiente affidarsi all'autenticazione a singolo fattore, come nome utente e password. L'autenticazione multifattore (MFA) offre un livello aggiuntivo di verifica e sicurezza, assicurando che solo gli utenti autorizzati possano accedere alle applicazioni business-critical.

L'autenticazione multifattore è un requisito imprescindibile. L'utilizzo di credenziali semplici, insieme a password e nomi utente ripetuti tra più applicazioni, aumenta significativamente la superficie soggetta agli attacchi di un'azienda.

Una volta autenticato e autorizzato l'utente tramite il metodo MFA, l'accesso SSO (Single Sign-On) consente di accedere a tutte le applicazioni desiderate con un unico set di credenziali, aumentando, di conseguenza, la produttività, poiché non è necessario riconfermare l'identità per ogni applicazione e si evitano problemi di sincronizzazione tra le applicazioni. Cambiare continuamente le decisioni rispetto a una vasta serie di segnali, tra cui il metodo MFA e l'accesso SSO alle applicazioni IaaS, in sede e SaaS, offre all'azienda una migliore protezione, fornendo, al contempo, una maggiore comodità per gli utenti finali.

Utilizzare la protezione avanzata dalle minacce contro attacchi di phishing, malware zero-day ed esfiltrazione dei dati basata su DNS

Nonostante l'ampia adozione di una strategia di sicurezza multilivello da parte delle aziende, i malintenzionati continuano a introdursi nei sistemi aziendali sfruttando i punti deboli dei sistemi di sicurezza. Anche con l'implementazione di firewall, gateway web protetti, sandbox, sistemi anti-intrusione e antivirus sull'endpoint, le aziende sono esposte e cadono nella trappola di attacchi di phishing, malware zero-day ed esfiltrazione dei dati basata su DNS. Allora cosa manca alle aziende?

Il DNS è un vettore spesso trascurato e i cybercriminali hanno sviluppato un malware specificamente concepito per sfruttare questa falla presente nei sistemi di sicurezza, eludendo i livelli di sicurezza esistenti per infiltrarsi nella rete ed esfiltrare i dati. L'aggiunta di un livello di sicurezza in grado di sfruttare il protocollo DNS è fondamentale; utilizzando questa fase di query iniziale come punto di controllo della sicurezza, una soluzione di sicurezza DNS può rilevare e fermare in anticipo gli attacchi informatici nella kill chain, proteggendo proattivamente l'azienda.

Le aziende devono sfruttare il protocollo DNS come punto di controllo della sicurezza per individuare e fermare in anticipo gli attacchi informatici nella kill chain.

Monitorare il traffico e le attività legate a Internet

Le aziende devono partire dal presupposto che l'ambiente circostante è ostile: questo è il principio fondamentale del modello Zero Trust. Pertanto, le organizzazioni devono impegnarsi a controllare e confermare tutte le attività, senza consentirle indiscriminatamente. A tal proposito, le aziende necessitano di visibilità sulle attività eseguite sulle proprie reti, con una vasta quantità di traffico e intelligence per effettuare confronti pertinenti.

Le aziende devono monitorare e verificare tutte le richieste DNS da parte dei dispositivi all'interno e all'esterno delle proprie reti (originate da laptop, telefoni cellulari, computer desktop, tablet, Wi-Fi guest o dispositivi IoT) per assicurarsi che le query non vengano indirizzate a siti dannosi o inaccettabili. Le organizzazioni necessitano anche della capacità di esaminare il comportamento del traffico, per cercare segnali di attività sospette, come la comunicazione con un server CnC (Command and Control) o l'esfiltrazione dei dati, avvisando immediatamente l'IT in caso di problemi. Una visione sul volume di traffico globale e sulle tendenze delle minacce semplifica per il personale IT l'individuazione di modelli irregolari o pericolosi.

Supportare l'integrazione con le funzionalità SIEM (Security Information and Event Management) e l'orchestrazione mediante le API RESTful

Le aziende possono avere centinaia o persino migliaia di applicazioni. Per implementare rapidamente le applicazioni in blocco e, allo stesso tempo, impostare i controlli relativi alle policy per gli accessi, è richiesta una configurazione tramite le API. Si tratta di una funzionalità cruciale per ogni ambiente applicativo su larga scala che cerca di migrare rapidamente da un sistema VPN tradizionale ad un accesso specifico per le applicazioni. L'adozione delle API continua ad aumentare man mano che le aziende adottano iniziative DevSecOps alla ricerca di attività di monitoraggio e configurazione disponibili tramite le API RESTful. Le aziende necessitano anche di plug-in per integrare i dati sulle minacce e sugli eventi nel SIEM per un ulteriore livello di indagine e correlazione. Un sistema scalabile deve, inoltre, integrarsi con le piattaforme di automazione dei workflow e la risoluzione delle minacce mediante la segnalazione nelle soluzioni di risposta e rilevamento degli endpoint di terze parti.

Conclusione

Poiché la trasformazione digitale è ormai una realtà, le aziende devono adottare un modello di sicurezza Zero Trust per favorire una corretta evoluzione delle loro attività in grado di garantire innovazione e flessibilità, senza compromettere la sicurezza. La protezione avanzata dalle minacce, l'accelerazione delle applicazioni, l'autenticazione MFA e l'accesso SSO su tutte le applicazioni (SaaS, in sede e IaaS) sono alcuni dei vantaggi principali derivanti dall'utilizzo di un ambiente Zero Trust. Un modello di sicurezza Zero Trust favorisce l'orchestrazione tramite le API, nonché l'integrazione con il sistema SIEM e le piattaforme di automazione dei workflow, fornendo visibilità su utenti e applicazioni e agevolando implementazioni su larga scala in tempi ridotti.

Akamai può aiutarvi a controllare l'evoluzione della rete e del sistema di sicurezza. Effettuate una valutazione Zero Trust costituita da sette domande per comprendere il livello di preparazione della vostra azienda in vista del passaggio ad un sistema di sicurezza Zero Trust. In seguito, vi verranno inviati i passaggi successivi personalizzati per la trasformazione della rete. In alternativa, potete consultare le risorse necessarie per avviare la trasformazione, visitando la pagina akamai.com/3waystozerotrust.

Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. L'Akamai Intelligent Edge Platform permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per l'edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24/7/365. Per scoprire perché i principali brand del mondo si affidano ad Akamai, visitate il sito https://www.akamai.com/it/it/ o https://blogs.akamai.com/it/ e seguite @AkamaiItalia su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo akamai.com/it/it/locations. Data di pubblicazione: 06/19.