Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 09/2016: 75.622
Diffusione 09/2016: 39.883
Lettori Ed. II 2016: 111.000
Quotidiano - Ed. nazionale

ItaliaOggi

Dir. Resp.: Pierluigi Magnaschi

16-DIC-2016
da pag. 5
foglio 1 / 2
www.datastampa.it

ItaliaOggi FOCUS

Cybersecurity: cruciale l'approccio "by design"

Prevenzione e difesa: il ruolo attivo di Almaviva contro le minacce informatiche

Negli ultimi 12 mesi più di un'attività su cinque nel mondo (21%) ha subito una forma di attacco cyber (nel 2015 erano il 15%), come rivelano i dati dell'International Business Report di Grant Thornton. Secondo la ricerca – che ha coinvolto 2.600 CEO e dirigenti in 37 economie del mondo - le estorsioni e le blackmail sono le forme più diffuse tra gli attacchi cyber rispetto alla frode di dati o di proprietà intellettuali. E nell'ultimo anno di fronte al cambiamento delle tipologie di minacce e reati cibernetici con effetti sulle persone, imprese e business, le risposte per proteggersi tendono a rimanere difensive.

Oggi più che mai, l'aumento della dipendenza economica e sociale dal Cyberspace - che da un lato offre nuove opportunità, dall'altro introduce nuove minacce – richiede capacità e strumenti adeguati a migliorare la sicurezza del sistema Paese. Ne parliamo con Antonio Amati, direttore generale Divisione IT di Almaviva, azienda italiana di ICT, che ha una struttura dedicata alla Cybersecurity.

"Reati come la frode e il furto di segreti industriali oggi possono essere commessi a distanza e su larga scala in pochi secondi. Possono colpire non solo le persone, ma anche le imprese o la Pubblica Amministrazione con effetti devastanti. Per questo sviluppare nuove capacità e nuovi strumenti rappresenta una sfida della massima importanza per la crescita e per il benessere e la sicurezza dei cittadini".

In questo contesto, l'emissione della direttiva NIS (Network and Information Systems) rappresenta un'opportunità nazionale?

"Senz'altro. Un'opportunità e una spinta importante verso un cambio di orizzonte culturale e di scenario tecnologico. Ancor oggi i temi di cybersecurity vengono spesso considerati degli elementi aggiuntivi (add-on) - applicativi o infrastrutturali – mentre sviluppano pienamente la loro efficacia quando sono previsti "by design". Concetto reso cogente anche nel nuovo General Data Protection Regulation (GDPR), oltre che da anni presente negli standard internazionali e nelle best practices di riferimento. Almaviva cura progetti e servizi ad alto contenuto di innovazione, portando le esperienze sui mercati della Pubblica Amministrazione, in ambito finanziario ed industriale, focalizzandosi sui nuovi paradigmi della Cybersecurity e proponendo un approccio "by design". Dalla Cyber Intelligence, alla gestione delle frodi, passando per il supporto alle transazioni sicure ed API management, raccogliendo le sfide tecnologiche mediante nuovi paradigmi di sviluppo e gestione dei servizi".

Quali asset propone Almaviva in tema di Cybersecurity?

"Gli asset innovativi sviluppati da Almaviva possono contare oggi su una piattaforma di sviluppo e di integrazione che utilizza metodologie e strumenti fortemente orientati ai mondi del mobile e dell'Internet of Things (IoT). Servizi ed applicazioni avanzate che garantiscono la sicurezza end to end delle informazioni. L'approccio alla sicurezza "by design" per la realizzazione di questi sistemi si rivela cruciale, tra l'altro, in termini di comunicazioni cifrate, attenzione alla gestione delle identità e delle autenticazioni, introduzione di protocolli di sicurezza e protezione delle informazioni sensibili che vengono scambiate nelle transazioni, con particolare attenzione all'ambito Finance e Banking".

Molti paesi stanno realizzando piani strategici nazionali che coinvolgono pubblico, privato e ricerca e puntano a rafforzare la difesa delle infrastrutture critiche nazionali, delle organizzazioni governative, delle aziende e dei singoli cittadini dagli attacchi cibernetici. Che ruolo può avere Almaviva in questa sfida?

"Sotto il profilo del contributo da portare al miglioramento delle capacità nazionali di gestione, Almaviva può concorrere alla prevenzione e difesa nell'ambito Cyberspace sulla base dell'esperienza accumulata negli anni nel settore della digitalizzazione di processi e servizi pubblici.
La consolidata cooperazione con la Pubblica Amministrazione ha contribuito ad elevare la connotazione di sicurezza dello spazio cibernetico e ne costituisce un prerequisito essenziale.
Il collegamento delle banche dati tra le pubbliche amministrazioni - non unificazione che si profilerebbe come limite strategico - può potenziare la capacità di contrasto alle frodi. La condivisione di informazioni di sicurezza può contribuire in modo decisivo ad elevare le capacità di difesa del Paese a fronte di minacce informatiche, compresa quella di matrice terroristica. A tale proposito è cruciale l'esercitazione operativa e l'incremento delle competenze Cybersecurity mediante sistemi di Cyber Test Range specifici. Un ulteriore elemento di salvaguardia dalla minaccia cyber di tipo terroristico, riguarda la protezione delle infrastrutture critiche, ambito in cui Almaviva ha maturato un'esperienza di valore, rilevante e continuativa, grazie al lavoro svolto al fianco di clienti che sovrintendono a questo genere di strutture. Il supporto fornito riguarda ogni tipo di esigenza nell'ambito dell'Information Technology e dei servizi di sicurezza attiva, sia di tipo fisico che di

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura 09/2016: 75.622
Diffusione 09/2016: 39.883
Lettori Ed. II 2016: 111.000
Quotidiano - Ed. nazionale

ItaliaOggi

Dir. Resp.: Pierluigi Magnaschi

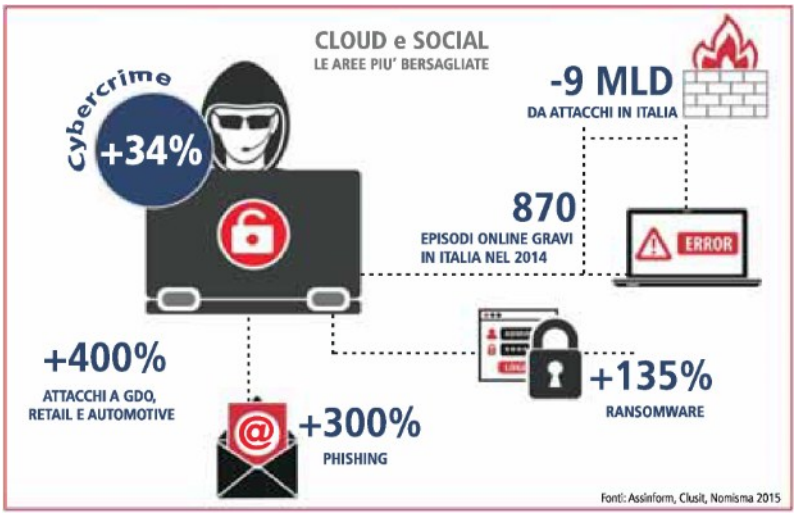
16-DIC-2016
da pag. 5
foglio 2 / 2
www.datastampa.it

tipo logico. In particolare, a livello applicativo, la diffusione di tecnologie legate alla mobilità, al Cloud e ai Big Data, richiede una attenzione specifica alla gestione sicura delle identità digitali, mediante processi e strumenti adeguati che consentano la profilazione dell'utenza, il corretto livello di autenticazione e quindi l'assegnazione dei diritti di accesso alle diverse risorse informatiche".

Al vertice Nato di Varsavia si è parlato della necessità di misure attive dedicate alla prevenzione degli attacchi…

"A livello preventivo, Almaviva si affida a un approccio basato su Open Source Intelligence (OSINT), mediante una piattaforma evoluta basata su algoritmi innovativi, che permette l'integrazione delle diverse forme di intelligence, per supportare al meglio analisti e manager nei cosiddetti CSIRT (Computer Security Incident Response Team), nelle diverse fasi di valutazione preventiva di attacco o nella ricerca di evidenze nell'analisi post incidente. La ricerca in linguaggio naturale, potenziata dall'uso di ontologie, e l'estensione della ricerca agli ambiti del deep e dark web, in aggiunta alle fonti aperte classiche (Web, Social, rss, feed, blog, forum), permettono di rilevare ed acquisire informazioni e segnali utili alla prevenzione o alla ricostruzione dettagliata di un attacco avvenuto. Naturalmente, una simile capacità di prevenzione andrebbe applicata anche a reti e sistemi SCADA che servono servizi primari, per poter introdurre contromisure necessarie alla resilienza".

Almaviva
www.almaviva.it



Antonio Amati
Direttore Generale Divisione IT