COMUNICATO STAMPA

Milano, 9 maggio 2017

Quasi la metà delle aziende italiane hanno subito un attacco alle applicazioni

Innumerevoli le vulnerabilità e i rischi che hanno causato danni al 46,9% delle imprese. In alcuni casi, fortunatamente pochi, gli attacchi hanno bloccato le applicazioni richiedendo oltre un mese di lavoro per ripristinare la quotidianità

Oggi a Milano alle ore 18 si tiene un workshop AIPSI -OAD per la presentazione del ***Rapporto OAD 2017 sugli attacchi agli applicativi***, una specifica verticalizzazione delle annuali indagini OAD sugli attacchi digitali in Italia.

L'indagine, sponsorizzata da F5 Networks quale Gold Sponsor del Rapporto OAD 2016, evidenza le innumerevoli vulnerabilità che sono sfruttate da cyber criminali e hacker malintenzionati, mettendo a rischio le aziende italiane: ben il **46,9%** di quelle che sono state coinvolte nel rapporto ha subito e rilevato attacchi agli applicativi, confermando che questo è uno dei principali problemi della sicurezza digitale insieme al comportamento ingenuo e scorretto degli utenti.

Fortunatamente, gli attacchi peggiori subito dalla maggiore parte delle aziende sono stati di basso livello, consentendo il ripristino dell'applicazione in poche ore, ma il **14,5%** di chi ha subito attacchi ha invece portato a conseguenze più gravi: fino a un mese per ritornare alla normalità. Addirittura per l'**1,8% il ripristino ha richiesto più di un mese di lavoro**.

Dal 18/5/2017 l'intero Rapporto sarà scaricabile dal sito web di AIPSI, www.aipsi.org, e di Malabo Srl, www.malaboadvisoring.it, la società dell'autore Marco R. A. Bozzetti, Presidente di AIPSI.

I principali dati emersi da Rapporto includono:

- **Il contesto: tipologia dei rispondenti e dei loro sistemi informatici**
    - così come per il Rapporto 2016, le aziende dei rispondenti appartengono in maggior parte a 3 settori merceologici: servizi ICT, manifatturiero, servizi professionali alle imprese; tutti gli altri settori ATECO considerati hanno avuto dei rispondenti, ma in numero limitato. La ripartizione per dimensioni come numero di dipendenti è ben bilanciata tra piccole, medie grandi e grandissime strutture. Il ruolo dei rispondenti è prevalentemente quello di Responsabile/Amministratore del sistema informatico e di responsabile di vertice dell'azienda/ente, soprattutto per quelle più piccole;

    - il numero totale di applicativi nel sistema informatico dipende dalle dimensioni e dal tipo di azienda: poco più della metà ha fino a 20 applicazioni, tipicamente le PMI, le grandi e grandissime aziende/enti ne hanno anche più di 100;
    - quasi tutti i rispondenti hanno applicazioni in produzione in cloud, ma solo pochi usano il cloud per i test alle applicazioni, sia funzionali sia tecnici.
- **Vulnerabilità degli applicativi**: innumerevoli sono i tipi di vulnerabilità, sfruttabili e sfruttati dagli attaccanti, dai bachi nel codice dovuti ad una programmazione non sicura al non settaggio dei parametri di sicurezza nelle configurazioni. Il grande numero di vulnerabilità degli applicativi e dei software che utilizzano, dai sistemi operativi al middleware, rende complessa e difficile l'analisi dei rischi (pratica ancora limitata ed effettuata prevalentemente da grandi aziende/enti) e la progettazione e realizzazione di efficaci ed efficienti misure di sicurezza, ma rende più facile portare attacchi agli applicativi con impatti sul business anche molto gravi.
- **Attacchi agli applicativi e relativi impatti**: poco meno della metà dei rispondenti, 46,9%, ha subito e rilevato attacchi agli applicativi, confermando che questo è uno dei principali problemi della sicurezza digitale (insieme al comportamento degli utenti). Gli impatti dell'attacco peggiore subito da un'azienda nell'anno, misurati in base al tempo necessario per ripristinare l'applicazione, sono stati nella maggior parte dei casi non gravi e l'applicazione e i suoi dati sono ripristinati in poche ore, ma per un significativo 14,5% dei rispondenti è occorso fino ad un mese solare per ripristinarla e per un piccolo, ma non trascurabile, 1,8%, più di un mese. Si rileva quindi che nel 2016 alcuni degli attacchi agli applicativi sono stati i più critici e difficili da ripristinare rispetto a tutti gli attacchi, non solo agli applicativi, occorsi nel 2015 ai rispondenti alle indagini OAD.
- **Principali cause** degli attacchi agli applicativi: dall'indagine è emerso che la causa più rilevante e diffusa è dovuta alle vulnerabilità dei software e delle infrastrutture usati dall'applicazione (36,2% nel 2016); al secondo posto la vulnerabilità intrinseca dell'applicativo stesso (25,4% nel 2016), dovuta allo sviluppo del codice in maniera non sicuro e/o con linguaggi non sicuri; seguono come causa le vulnerabilità dei sistemi di identificazione, autenticazione e controllo degli accessi (20,8% nel 2016).
- **Misure di sicurezza** in essere per gli ambienti applicativi dei rispondenti: i sistemi informatici dei rispondenti appartengono in gran parte alla fascia alta per le misure di sicurezza, grazie anche al fatto che molti sono di aziende di servizi ICT, le quali, quindi, hanno (o dovrebbero avere) sistemi informatici e relativa sicurezza allo stato ultimo dell'arte (ma anche tra le aziende ICT ci sono casi di "ciabattino con le scarpe rotte"). Il 70% dei rispondenti classifica dati ed applicazioni; più dell'84% gestisce in maniera centralizzata l'autenticazione ed il controllo degli accessi; prima di passare un'applicazione in produzione, l'80% effettua test funzionali e quasi il 69% test tecnici e sulla sicurezza del codice; quasi il 55% effettua penetration test.

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, è il Capitolo italiano della internazionale ISSA (www.issa.org)

Malabo Srl (www.malaboadvisoring.it) è la società dell'autore che ha ideato e realizzato l'indagine OAD ed il Rapporto

Per qualsiasi maggior informazione contattare: aipsi@aipsi.org