Oltre il 50% delle richieste di Incident Response avviene troppo tardi

Ago 30, 2019 Kaspersky Kaspersky Partner Space 0

Nel 2018, circa il 56% delle richieste di Incident Response (IR) prese in esame dagli esperti di sicurezza di Kaspersky è avvenuto solo quando le conseguenze dell'attacco subito erano ormai evidenti, come il trasferimento non autorizzato di denaro, le workstation criptate da ransomware e la mancata disponibilità del servizio. Il 44% delle richieste, invece, è stato elaborato nella fase iniziale dell'attacco evitando ai clienti di subire gravi conseguenze. Questi alcuni dei risultati del nuovo Incident Response Analytics Report di Kaspersky.

E' opinione comune che i servizi di Incident Response servano solo nei casi in cui un attacco informatico abbia già causato dei danni e ci sia bisogno di indagare in modo più approfondito. Tuttavia, analizzando diversi casi di Incident Response a cui, nel 2018, hanno partecipato gli esperti di sicurezza di Kaspersky è emerso che questo servizio può essere utilizzato non solo come strumento investigativo ma anche come strategia per rilevare un attacco durante la sua fase iniziale, in modo da prevenirne i danni.

Nel 2018, il 22% delle procedure di IR è stato avviato dopo il rilevamento in rete di un’attività potenzialmente pericolosa e un ulteriore 22% dopo che un file malevolo è stato rilevato all’interno della rete. Senza altri segni di violazione, entrambi i casi suggeriscono che ci sia un attacco in corso. Tuttavia, non tutti i team di sicurezza aziendale sono in grado di sapere se gli strumenti di sicurezza automatizzati abbiano già rilevato e bloccato l’attività malevola, o se sia solo l’inizio di un’operazione malevola più ampia e invisibile al’interno della rete per la quale si rende necessario l’intervento di specialisti esterni. A seguito di una valutazione errata, l’attività dannosa si trasforma in un grave attacco informatico con conseguenze reali. Nel 2018, il 26% degli casi esaminati in modo tardivo erano stati causati

da infezioni da encryption malware, mentre l'11% degli attacchi ha portato al furto di denaro. Il 19% dei casi tardivi sono stati il risultato del rilevamento di spam proveniente da un account di posta aziendale, del rilevamento di indisponibilità del servizio o di una violazione avvenuta con successo.

"Questa situazione indica che in molte aziende è necessario migliorare i metodi di rilevamento e le procedure di Incident Response. Rilevare un attacco nella sua fase iniziale vuol dire contenere la portata delle conseguenze. In base alla nostra esperienza, però, le aziende spesso non prestano la dovuta attenzione agli artefatti di un attacco serio, e contattano il gruppo di Incident Responde quando è già troppo tardi per prevenire i danni. D'altro canto, abbiamo constatato che molte aziende hanno imparato a valutare i segni di un grave attacco informatico nella loro rete e questo ci ha consentito di prevenire quelli che sarebbero potuti diventare incidenti pericolosi. Invitiamo quindi le altre organizzazioni a considerare questi come case study di successo", ha commentato Ayman Shaaban, Security Expert di Kaspersky.

Ulteriori risultati del report:

- Nell'81% delle reti interne delle organizzazioni che hanno fornito i dati per questa analisi sono stati rilevati indicatori di attività malevola
- Nel 34% delle organizzazioni sono stati rilevati segni di un attacco mirato avanzato
- Il 54,2% delle organizzazioni finanziare è stato attaccato da uno o più gruppi APT (Advanced Persistent Threat).

Per rispondere efficacemente agli incidenti di sicurezza, Kaspersky

raccomanda:

- Assicurarsi che l’azienda abbia un team interno dedicato (almeno un dipendente) responsabile della sicurezza informatica
- Implementare sistemi di backup per le attività critiche
- Per rispondere in modo tempestivo ad un attacco informatico, schierare in prima linea il gruppo interno di IR e rivolgersi ad esperti esterni per gli incidenti più complessi
- Sviluppare un piano IR con linee guida e procedure dettagliate per i diversi tipi di attacco
- Introdurre corsi di sensibilizzazione per educare i dipendenti alle tematiche di “igiene digitale” e spiegare come riconoscere ed evitare email o link potenzialmente dannosi
- Implementare procedure di gestione delle patch per l’aggiornamento del software
- Condurre regolarmente dei security assessment dell’infrastruttura IT dell’azienda

La versione completa del report è disponibile su Securelist.com.

Condividi l’articolo

Google estende il bug bounty alle app più popolari su Google Play

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/08/30/oltre-il-50-delle-richi

este-di-incident-response-avviene-troppo-tardi/