IBM Italy News Room

IBM annuncia X-Force Red, il nuovo team per il Security Testing

L’azienda amplia il team con l’ingresso di esperti di fama mondiale e continua l’espansione delle sue attività di consulenza e servizi dedicati alla sicurezza

ARMONK, NY - 02 ago 2016: IBM Security ha annunciato oggi la creazione di IBM X-Force Red, un team di professionisti della sicurezza e di hacker etici con l’obiettivo di aiutare le aziende a identificare le vulnerabilità presenti nelle proprie reti informatiche, nell’hardware e nelle applicazioni software, in anticipo rispetto ai pirati informatici. Il team, parte integrante di IBM Security Services, verificherà anche le vulnerabilità di sicurezza legate al fattore umano e relative ai processi e alle procedure quotidiane, che gli aggressori spesso utilizzano per eludere i controlli di sicurezza. Guidato da Charles Henderson di IBM, esperto di fama mondiale nel campo dei penetration test, IBM X-Force Red è un team globale, costituito da un network di centinaia di professionisti della sicurezza basati in diverse località in tutto il mondo, tra cui gli Stati Uniti, il Regno Unito, l’Australia e il Giappone.

I professionisti nel security testing che fanno parte di IBM X-Force Red portano con sé un patrimonio di competenze maturato in molteplici settori, quali sanità, servizi finanziari, retail, produzione e settore pubblico. Nel loro insieme, hanno condotto test di sicurezza per i più importanti brand e pubbliche amministrazioni del mondo, quali penetration test, hacking etico, social engineering e test di sicurezza fisica. L’attività di IBM X-Force Red si avvale della security intelligence di IBM X-Force Research, della piattaforma di condivisione delle minacce IBM X-Force Exchange e di IBM Security AppScan per fornire un ulteriore livello di security testing basato anche su esperienza, intuizioni e creatività delle persone.

Gli attacchi dolosi contro le risorse aziendali sono in aumento, con il 64 per cento di incidenti in più segnalati nel 2015 rispetto al 2014.[1] Tuttavia, quando vengo rilasciate nuove soluzioni online, la sicurezza è spesso un aspetto trascurato. Ad esempio, uno studio IBM ha riscontrato che il 33 per cento delle aziende non esegue test sulle applicazioni mobili per ricercare eventuali vulnerabilità di sicurezza.[2] Gli aggressori che ricercano gli exploit zero-day per i propri attacchi analizzano invece costantemente le tecnologie esistenti, che pertanto richiedono una verifica periodica della sicurezza per garantire un’adeguata protezione.

“Avere a disposizione un mezzo di scansione automatica dei propri server e del codice sorgente è certamente un notevole aiuto nella prevenzione delle violazioni dei dati, ma nei security testing non va trascurato l'elemento umano,” ha dichiarato Charles Henderson, Global Head of Security Testing and X-Force Red, IBM Security. “I migliori esperti nel testing possono apprendere come funziona un determinato ambiente e creare modalità uniche di attacco utilizzando tecniche ancora più sofisticate di quelle a disposizione dei criminali. IBM X-Force Red offre alle organizzazioni la possibilità di operare con agilità senza creare punti morti nella propria struttura di sicurezza.”

Le quattro aree di focalizzazione di IBM X-Force Red sono:

- **Applicazioni** – penetration testing e revisione del codice sorgente per identificare le vulnerabilità di sicurezza nelle varie piattaforme (web, applicazioni mobili, terminali, mainframe e middleware).

- **Rete** – penetration testing delle frequenze interne, esterne, wireless e delle frequenze radio di altro tipo.

- **Hardware** –verifica della sicurezza tra gli ambienti fisici e digitali attraverso test dell'Internet of Things (IoT), dei dispositivi wearable, dei sistemi POS, dei bancomat, dei sistemi automotive e dei kioski self-service.

- **Fattore umano** – esecuzione di simulazioni di phishing, di social engineering, di ransomware e di violazioni della sicurezza fisica per determinare i rischi legati al comportamento umano.

IBM X-Force Red fornisce servizi di security testing secondo tre modelli: singoli progetti, attività di test in abbonamento e programmi di testing gestiti. Il modello in abbonamento offre una significativa flessibilità di budget, permettendo di allocare preventivamente determinate risorse economiche per i test senza dover definire in anticipo obiettivi specifici per gli stessi e nemmeno le tipologie di test richieste. I programmi di verifica gestiti sono ideali per le organizzazioni che non dispongono di personale dedicato alla sicurezza per determinare le priorità di test, documentare i requisiti correttivi e far applicare i necessari criteri.

Tutti i modelli includono funzioni di analisi delle vulnerabilità, progettate per migliorare l'efficienza e l'impatto dei programmi di security testing. Questo approccio agile offre alle aziende una maggiore flessibilità di spesa per la sicurezza e potenti funzionalità di test su richiesta, tra cui la valutazione e la gestione delle vulnerabilità per l'intero ciclo di vita delle applicazioni e dei deployment di rete.

Informazioni su IBM Security

IBM Security offre un portfolio di offerta di servizi e prodotti per la sicurezza tra i più avanzati e integrati a livello enterprise. Questo portfolio, supportato dalla ricerca di fama mondiale condotta da IBM X-Force®, consente alle organizzazioni di gestire il rischio in modo efficace e di difendersi dalle minacce emergenti. IBM gestisce una delle più vaste organizzazioni al mondo di ricerca, sviluppo e delivery dedicata alla sicurezza, monitora 35 miliardi di eventi di sicurezza ogni giorno in oltre 130 paesi e detiene oltre 3.000 brevetti relativi alla security. Per ulteriori informazioni, visitate www.ibm.com/security, seguite @IBMSecurity su Twitter oppure visitate il blog di IBM Security Intelligence.

- *X-Force IBM Cyber Security Intelligence Index, aprile 2016*

The State of Mobile Application Insecurity, marzo 2015
