7 trend sulla cybersecurity da tenere d’occhio nel 2018

Gli esperti di sicurezza informatica di tutto il mondo hanno previsto che il devastante effetto dei costi del crimine informatico raggiungerà i 6 trilioni di dollari entro il 2021, a meno che non vengano adottate misure adeguate. In questo quadro sempre più critico, governi ma soprattutto le aziende cercano di capire come proteggersi al meglio dal volume crescente e dalla complessità degli attacchi informatici.

Di seguito sono riportati 7 trend da tenere d’occhio per quel che riguarda la sicurezza informatica quest’anno.

1) GDPR e privacy

La protezione dei dati è una preoccupazione critica in un mondo sempre più digitale e il 25 maggio 2018 è un punto di svolta per la protezione dei dati in Europa. Essa segna la fine del periodo transitorio per il regolamento generale sulla protezione dei dati dell’UE (GDPR) in quanto diventa applicabile per legge. La mancata conformità potrebbe comportare multe fino al 4% del fatturato globale alle aziende, una somma significativa che richiede attenzione.

2) Internet of Things e le botnet

Nel 2016, Mirai ha dimostrato che i dispositivi Internet of

Things (IoT) possono essere effettivamente utilizzati come **botnet**. Oggi, lo sviluppo del prodotto, le considerazioni sul *time to market* e i vincoli tecnici di potere lasciano i dispositivi IoT esposti a vulnerabilità critiche. L'impatto delle violazioni dei dati si estende ora anche a questi sistemi in quanto sono direttamente collegati alla rete. È ampiamente accettato che lo stato della sicurezza IoT sia scarso. Un vero rischio date le previsioni che prevedono oltre 500 dispositivi connessi nelle nostre case entro il 2022.

3) L'industria 4.0, nuovo settore suscettibile gli attacchi informatici

L'industra 4.0 sta già trasformando l'industria e le infrastrutture globali, promettendo maggiore efficienza, produttività e sicurezza. Competere significa spostare le apparecchiature di processo online, esponendo spesso involontariamente le vulnerabilità dei componenti agli attacchi informatici. Gli stabilimenti di produzione sono contenitori ricchi di proprietà intellettuale, segreti commerciali e informazioni ingegneristiche. Gli attacchi alle infrastrutture pubbliche sono motivati □□dal guadagno finanziario e dall'hacktivismo.

4) Il tempo il peggior nemico della sicurezza

I recenti attacchi informatici a organizzazioni di alto profilo stanno dimostrando che, contro i cybercriminali sofisticati, i controlli preventivi da soli non sono

sufficienti. Oggi, occorrono in media oltre 191 giorni per rilevare una violazione dei dati. Quanto più tempo è necessario per rilevare e rispondere alle minacce, tanto maggiore è il danno finanziario e di reputazione arrecato all'organizzazione dall'incidente. A causa dell'enorme crescita dei dati dei registri di sicurezza, delle limitazioni delle tecnologie, dell'uso inefficace dell'intelligence delle minacce, dell'incapacità di monitorare i dispositivi IoT e della carenza di talenti della sicurezza informatica, le organizzazioni sono esposte a tempi di sosta costosi.

5) Il ruolo dell'Intelligenza Artificiale

Mentre le organizzazioni subiscono una trasformazione digitale, c'è un crescente volume di attacchi informatici sempre più sofisticati e persistenti. I malware stanno diventando sempre più intelligenti, in grado di adattarsi "in modo intelligente" e di eludere le tradizionali misure di rilevamento. Con una carenza globale di talenti della sicurezza informatica, le organizzazioni stanno perdendo la corsa agli armamenti informatici. Il volume dei dati di sicurezza supera di gran lunga la nostra capacità legacy di utilizzarlo in modo efficace, portando a un numero crescente di casi d'uso della sicurezza informatica abilitati all'Intelligenza Artificiale, in quanto questa tecnologia ci permette di:

- accelerare il rilevamento e la risposta degli incidenti;
- una migliore identificazione e comunicazione dei rischi per l'azienda;
- fornire una visione unificata dello stato della sicurezza all'interno dell'organizzazione.

7) Password sostituite dall’autenticazione biometrica

Le nostre vite digitali sono governate da una complessa rete di app online ognuna delle quali richiede un nome utente e una password per controllare l’accesso. Per proteggere i dati dietro queste app, selezionare password oscure e complesse e cambiarle spesso, è una buona pratica, ma anche piuttosto rara. Con miglioramenti esponenziali della potenza di calcolo e un facile accesso a molte di esse nel cloud, il tempo necessario per hackerare le password a si sta rapidamente riducendo. Ciò che ha richiesto quasi 4 anni nel 2000, ora richiede solo 2 mesi. Di conseguenza, è sempre più comune incontrare l’autenticazione biometrica (facciale, impronta digitale, diaframma e voce) inclusa nei dispositivi mobili, tablet e laptop di tutti i giorni, oltre all’accesso fisico e ai servizi online.

8) Le industrie più colpite: sanità ed energia

La maggior parte degli attacchi informatici intrapresi da organizzazioni criminali sono motivati dal denaro. Il valore delle informazioni sul deep web varia in base alla domanda, disponibilità, completezza e dalla capacità di riutilizzo. Di conseguenza, le informazioni sanitarie e finanziarie personali sono molto ricercate. Le cartelle cliniche possono fruttare fino a 1.000 dollari, a seconda di quanto sono completi. Altri attacchi informatici hanno motivi politici e nazionali, qui la rottura dei servizi critici attraverso gli attacchi al settore

energetico è un rischio chiave nel 2018; come evidenziato dalle recenti notizie della campagna hacker russa contro la rete elettrica degli Stati Uniti, che si sospetta sia in corso da diversi anni.

The post 7 trend sulla cybersecurity da tenere d’occhio nel 2018 appeared first on Key4biz.

https://www.key4biz.it/7-trend-sulla-cybersecurity-da-tenere-docchio-nel-2018/220833/