

Hackerata Suprema. Gli esperti: “Società di (in)sicurezza biometrica”

Ago 16, 2019 Marco Schiaffino Attacchi, Gestione dati, Hacking, In evidenza, Leaks, News, RSS, Scenario, Vulnerabilità 1

La vittima è Suprema, che gestisce la piattaforma di sicurezza Bio Star 2. Rubate impronte digitali e le credenziali di amministrazione.

Utilizzare un sistema di riconoscimento facciale e scansione delle impronte digitali per regolare l'accesso agli edifici e controllare gli spostamenti al loro interno può sembrare la soluzione per “blindare” la sede di un'azienda.

Se chi gestisce i sistemi ha però un'infrastruttura informatica che è un colabrodo, però, rischia di essere tutto inutile. Anzi: a ben guardare può trasformarsi in un boomerang.

È successo ai clienti di **Suprema**, una società sud coreana specializzata nella fornitura di sistemi di sicurezza basati sull'analisi biometrica e che ha recentemente avviato una partnership per integrare i suoi sistemi di controllo in **AEOS**, un sistema di controllo venduto da **Nedap**.

Come spiegano **Noam Rotem** e **Ran Locar**, ricercatori della società di sicurezza **vpnMentor**, Suprema è stata vittima di un attacco hacker che ha portato a un clamoroso leak di dati relativi alla sua piattaforma **Bio Star 2**.

I 23 gigabyte di dati individuati dai due analisti, che i

pirati informatici hanno “estratto” dai sistemi di Suprema, comprendono 27,8 milioni di record, tra cui un milione di impronte digitali di dipendenti delle aziende che usano i sistemi Bio Star 2, i dati di riconoscimento facciale e i log di accesso.

Non solo: i cyber-criminali sono riusciti anche a mettere le mani sulle credenziali di amministrazione del sistema. **Un compito non troppo difficile, per la verità, visto che secondo i ricercatori le credenziali erano conservate in chiaro, senza l'uso di hashing o crittografia.**

Gli hacker che hanno violato i sistemi di Suprema, in pratica, hanno a disposizione tutto quello che gli serve per modificare gli account esistenti o crearne di nuovi. **In altre parole: possono superare i sistemi di sicurezza di circa 5.700 organizzazioni in 83 paesi diversi.**

La parte più sconcertante, però, riguarda alcuni elementi che emergono dal report pubblicato sul sito ufficiale di vpnMentor, come il fatto che la maggior parte delle password avesse un livello di sicurezza ridicolo, con credenziali che

comprendevano le solite “Password” e “abcd1234”.

Anche il livello di reattività di Suprema, secondo i ricercatori, lascia parecchio a desiderare. **Dopo aver inviato numerose email, Rotem e Locar sarebbero stati addirittura “rimbalzati” al telefono da un impiegato di Suprema.**

La situazione si è risolta solo quando i due esperti di sicurezza sono riusciti a contattare la sede francese dell’azienda, dove hanno trovato una maggiore collaborazione.

Tutta la vicenda, però, accende i riflettori anche su un altro aspetto collegato all’uso di sistemi biometrici. A differenza di quanto accade con le normali credenziali, infatti, i sistemi di autenticazione come le impronte digitali o il riconoscimento facciale scontano un “piccolissimo” svantaggio: non possono essere modificate.

Una volta che sono state rubate, non c’è più nulla da fare se non cambiare sistema di autenticazione. Una considerazione che dovrebbe far riflettere chi sta considerando di battere questa via per sostituire l’utilizzo di password e PIN.

Condividi l’articolo

Quattro app per appuntamenti rivelano l’esatta posizione degli utenti

Articoli correlati

Altro in questa categoria

<https://www.securityinfo.it/2019/08/16/hackerata-suprema-gli-esperti-societa-di-insicurezza-biometrica/>