Secure Authentication: Zet jouw cybersecurityhelm op

In ijshockey, waar spelers elkaar raken met snelheden van 30 km/u en schoten lossen tot wel 161 km/u, is het moeilijk voor te stellen dat spelers tot eind jaren 70 zonder helm speelden. Sindsdien heeft dit essentiële stukje veiligheidsuitrusting het aantal verwondingen aanzienlijk verminderd en de carrières van professionele spelers verlengd.

Dit voorbeeld laat zien dat de oplossing voor een pijnlijke uitdaging soms verrassend eenvoudig kan zijn. Dit geldt ook voor authenticatie, een favoriete aanvalsmethode van kwaadwillenden. Data toont keer op keer aan dat een enkel wachtwoord, hoe sterk ook, niet langer voldoende is. Een extra beveiligingslaag – multi-factor-authenticatie (MFA) – vermindert de kans op succesvolle aanvallen op gebruikersreferenties aanzienlijk.

Goed ontwikkelde processen om de authenticatie van werknemers te beveiligen, gecombineerd met wachtwoordhygiëne, zijn essentiële onderdelen van een preventieve strategie die aanvallen stopt voordat ze schade kunnen aanrichten. Om deze aanpak te ondersteunen, heeft ESET zijn cloudgebaseerde MFA-oplossing ESET Secure Authentication geïntegreerd in de ESET PROTECT Hub – een nieuw centraal toegangspunt tot het ESET PROTECT Platform, dat ook MSP's ondersteunt met gebruikers-, licentie- en hiërarchiebeheertools.

Gericht op kwetsbare punten

Net zoals ijshockeyspelers vaak mikken op de bovenhoeken van het doel vanwege het succespercentage, weten cybercriminelen dat referenties tot de meest kwetsbare lagen van bedrijfsbeveiliging behoren vanwege de menselijke factor. Ondanks de groeiende wereldwijde bewustwording over cybersecurity blijft "123456" bijvoorbeeld het meest gebruikte wachtwoord.

Dit probleem beperkt zich niet tot het grote publiek. Ook bij IT-beheerders is slechte wachtwoordhygiëne een veelvoorkomend probleem. Onderzoek naar meer dan 1,8 miljoen geïdentificeerde beheerdersportals in 2023 onthulde dat 40.000 hiervan "admin" als wachtwoord gebruikten. Het is dan ook geen verrassing dat volgens het Verizon Data Breach Investigations Report 2024, 77% van de aanvallen op webapplicaties te maken had met gestolen referenties. Maar liefst 21% hiervan was het resultaat van brute force-aanvallen op eenvoudig te raden wachtwoorden, terwijl 13% zwakke plekken uitbuitte.

Terwijl bedrijven worstelen met de wachtwoordluiheid van werknemers, blijven tegenstanders hun technieken verbeteren om zelfs de meest waakzame en technisch onderlegde gebruikers te misleiden. Denk bijvoorbeeld aan AI-gedreven phishingaanvallen of krachtige computers die willekeurige wachtwoorden van zes tekens binnen een dag kunnen kraken, ondanks verbeterde hashing-methoden. Gebruikers van oudere hashing-methoden lopen nog meer risico.

Het belang van een MFA-helm

Gelukkig gedragen de meeste aanvallers die op referenties mikken zich als wanhopige ijshockeyspelers die pucks vanaf de andere kant van de ijsbaan op het doel schieten in de hoop op succes. Deze "spray-and-pray"-tactieken zijn nog steeds gangbaar. Volgens Microsoft-gegevens uit 2023 vormen eenvoudige, goedkope en massaal geproduceerde wachtwoordaanvallen de meerderheid. Microsoft weerstaat meer dan 1.000 wachtwooraanvallen per seconde. Meer dan 99,9% van de gecompromitteerde accounts had geen MFA ingeschakeld. Google ontdekte in een onderzoek uit 2019 soortgelijke resultaten: een eenvoudige extra verificatiestap kan 100% van

geautomatiseerde bots, 99% van grootschalige phishingaanvallen en 66% van gerichte aanvallen blokkeren.

Meervoudige of aanvullende verificatiefactoren zijn inmiddels een standaard compliance-eis geworden, net zoals een helm verplicht is in ijshockey.

Geautomatiseerde aanvallen op referenties:

- **Phishing** – Frauduleuze berichten die gebruikers misleiden om hun inloggegevens te delen.
- **Password spraying** – Veelgebruikte wachtwoorden zoals “wachtwoord” of “1234” uitproberen tegen grote aantallen accounts.
- **Woordenboekaanvallen** – Wachtwoorden uit een woordenboek proberen op een geldig account.
- **Brute force** – Automatische aanvallen op een enkel account met alle mogelijke wachtwoordcombinaties.
- **Credential stuffing** – Hergebruik van gelekte referenties uit eerdere datalekken op meerdere accounts.

Bescherming zonder gedoe

Beschikbaar in de hogere niveaus van ESET PROTECT biedt ESET Secure Authentication een extra beveiligingslaag tegen veelvoorkomende aanvallen op referenties. Het beschermt zowel werknemers als IT-beheerders bij het inloggen op bedrijfssystemen, vermindert het risico op gestolen en gecompromitteerde referenties, voorkomt toegang tot bedrijfsdata door kwaadwillenden en helpt bedrijven te voldoen aan compliance-eisen.

En het beste van alles: eenvoud in gebruik. De implementatie duurt ongeveer 10 minuten in de cloud. ESET Secure Authentication heeft geen speciale hardware nodig, is eenvoudig schaalbaar en ESET verzorgt het onderhoud en de upgrades.

Veilig met ESET

Het misbruiken van geldige accounts blijft de weg van de minste weerstand voor cybercriminelen, volgens het IBM X-Force Threat Intelligence Index 2024. Ondanks dat effectieve bescherming beschikbaar is, maken veel bedrijven hier nog steeds geen gebruik van.

Gezien de voortdurende aanvallen op zakelijke accounts, is het tijd om “een helm op te zetten”. Met ESET PROTECT kunnen bedrijven niet alleen profiteren van gelaagde en AI-gestuurde bescherming tegen geavanceerde aanvallen, maar ook eenvoudig MFA inzetten om hun kostbare accounts te verdedigen tegen massale geautomatiseerde aanvallen.