Wirksamer Schutz von Online-Diensten und Reputation

Kaspersky Takedown Service

kaspersky BRING ON THE FUTURE

> 500

Millionen versuchte Zugriffe auf betrügerische Webseiten wurden von Kaspersky-Forschern im Jahr 2022 gestoppt

20.000 $

betragen die durchschnittlichen Kosten für schädliche Apps auf Google Play im Dark Web

36,3%

aller Phishing-Angriffe, die 2022 von Kaspersky Anti-Phishing-Technologien erkannt wurden, betrafen Finanzdaten

Die Herausforderung

Cyberkriminelle erstellen bösartige und Phishing-Domains sowie Social-Media-Konten, um Ihr Unternehmen und Ihre Marken anzugreifen. Diese Bedrohungen müssen sofort nach ihrer Entdeckung bekämpft werden. Andernfalls kann es zu Umsatzeinbußen, Rufschädigung, Verlust des Kundenvertrauens, Datenlecks und vielem mehr kommen. Allerdings ist ein Domain-Takedown ein komplexer Prozess, der Fachkenntnis und Zeit erfordert.

Über den Kaspersky Takedown Service

Kaspersky Takedown Service

Kaspersky blockiert mehr als 15.000 betrügerische / Phishing-URLs und verhindert täglich über eine Million Versuche, solche URLs anzuklicken. Der Service wehrt Angriffe durch schädliche Social-Media-Konten schnell ab, bevor Ihr Unternehmen Schaden nimmt. Wir kümmern uns um das Takedown-Management und ermöglichen eine schnelle Reaktion zur Minimierung Ihres digitalen Risikos, damit sich Ihr Team auf andere wichtige Aufgaben konzentrieren kann.

Durch die Zusammenarbeit mit internationalen Organisationen sowie nationalen und regionalen Strafverfolgungsbehörden bietet Kaspersky seinen Kunden einen wirksamen Schutz ihrer Online-Dienste und ihres guten Rufs:

- INTERPOL
- Europol
- Microsoft Digital Crimes Unit
- Die Nationale Einheit für Hightech-Kriminalität (NHTCU) der niederländischen Polizeibehörde
- City of London Police
- Weltweite Computer Emergency Response Teams (CERTs)

Funktionsweise

1

Anfragen können über den Kaspersky Company Account gestellt werden, unser Support-Portal für Unternehmenskunden.

2

Wir bereiten alle notwendigen Unterlagen vor und senden den Takedown-Antrag an die zuständige lokale/regionale Behörde (CERT, Registrierungsstelle usw.), die über die notwendigen Rechte zur Deaktivierung der Domain verfügt.

3

Sie werden über jeden Schritt informiert, bis die angeforderte Ressource erfolgreich deaktiviert wurde.

Die Vorteile auf einen Blick

Weltweite Abdeckung

Es spielt keine Rolle, wo eine schädliche oder Phishing-Domain registriert ist, Kaspersky wird bei der regionalen Organisation mit der entsprechenden rechtlichen Befugnis einen Takedown anfordern.

End-to-End-Management

Wir kümmern uns um den gesamten Takedown-Prozess und minimieren Ihre Beteiligung

Integration mit Digital Footprint Intelligence

Der Kaspersky Takedown Service kann auch separat erworben werden. Hohe Synergieeffekte erzielen Sie aber durch die Integration mit Kaspersky Digital Footprint Intelligence. Mit Kaspersky Digital Footprint Intelligence werden Sie in Echtzeit über Phishing- und Malware-Domains informiert und können diese direkt vom Kaspersky Takedown Service sperren lassen.

Vollständige Sichtbarkeit

Sie werden in jeder Phase des Prozesses benachrichtigt, von der Registrierung Ihrer Anfrage bis zum erfolgreichen Takedown.

Kaspersky Digital Footprint Intelligence

Der Service wurde entwickelt, um Kunden einen Überblick über ihren Fußabdruck in offenen Netzen zu bieten und aufzuzeigen, welche Möglichkeiten ihre digitale Präsenz Angreifern bietet

Kaspersky Takedown Service

Mehr erfahren

www.kaspersky.de

#kaspersky
#bringonthefuture