

Dark Web Monitoring zum Schutz vor Daten- missbrauch

#stopcybercrime

- Was ist ein Dark Web Monitoring?

Mehr als die Hälfte aller Unternehmen sind von Datenmissbrauch im Dark Web betroffen. Mit unserem Dark Web Monitoring schützen wir Unternehmen davor, dass sich Unbefugte Zugang zu den Firmendaten oder der gesamten IT-Infrastruktur verschaffen. Dafür scannen unsere eigens entwickelten Suchmaschinen rund um die Uhr Tausende von Plattformen im Dark Web. Sobald ein Breach auftritt, erhalten Sie umgehend automatisiert eine E-Mail mit allen bekannten Informationen zu dem Treffer. So haben Sie die Möglichkeit, rechtzeitig zu reagieren und die Passwörter in Ihrem Unternehmen zu ändern.

Was passiert im Dark Web?

Das Dark Web ist ein unregulierter Teil des Internets, der absichtlich versteckt wird und über Standard-Webbrowser nicht zu erreichen ist. Er wird nicht überwacht und folgt keinen Regeln oder Gesetzen. Auf der „hellen“ Seite nutzen das Dark Web z.B. Menschen, die sich frei von Zensur oder der Angst vor Verfolgung austauschen möchten. Die dunkle Seite hingegen ist tatsächlich düster. Hier tummeln sich Marktplätze für Drogen- oder Waffenhandel, Kreditkartenbetrug, Dokumentenfälschung, Glücksspiel, illegale Pornografie, bösartige Viren und Schnüffelprogramme. Eine Oase für Cyberkriminelle zum Verkauf von geklauten Daten.



- **Wie gelangen Daten ins Dark Web?**
Mobilfunkanbieter, Online-Händler, Bezahldienste, Multi-
mediaportale, Softwarefirmen und Mailhosts – kein System
ist vor Hackern sicher. Oft haben sie es auf den millionen-
fachen Raub von Kundendaten abgesehen. Grundsätzlich
kann jeder Onlinedienst Ziel einer solchen Attacke werden.
Die Daten bieten die Cyberkriminellen daraufhin unver-
schlüsselt zur freien Verfügung oder zum Kauf in Foren im
Dark Web an. Aktuell sind über 25 Mrd. Zugangsdaten im
Dark Web zu finden und es werden stetig mehr. Darunter
Benutzer-Passwort-Kombinationen und andere Zugangs-
daten von Menschen in Unternehmen.

Wie kann ich mein Unternehmen davor schützen?

Im ersten Schritt sollten Sie nie dasselbe Passwort für ver-
schiedene Dienste verwenden und Ihre Kennwörter regel-
mäßig ändern. Nutzen Sie hierfür am besten einen Pass-
wortmanager. Im zweiten Schritt empfehlen wir unser Dark
Web Monitoring. Unsere Suchmaschinen scannen selbst
die finstersten Ecken gründlich. Sie erhalten proaktiv eine
E-Mail-Benachrichtigung, wenn Passwörter, Zugangsdaten,
uvm. zur Domäne des Unternehmens gefunden wurden. Der
Betroffene kann daraufhin umgehend Passwörter und Zu-
gangsdaten ändern und die gestohlenen Daten für Cyber-
kriminelle unbrauchbar machen. Diese Funktion schützt
davor, dass sich Unbefugte Zugang zu Firmendaten oder zur
gesamten IT-Infrastruktur verschaffen.



Möchten Sie wissen, ob Ihre Firmendomain und E-Mail-Adresse im Dark Web zum Verkauf angeboten werden? Jetzt kostenfreien Dark Web Monitoring Report beantragen. Schicken Sie uns einfach Ihre Domain und Ihre Kontaktdaten, unter denen wir Sie für die Auswertung erreichen können, per E-Mail an info@anqa-itsecurity.de.



- Unser Sales Team berät Sie gerne zu unseren IT-Sicherheitslösungen +49 2203 202 07-80