WERDEN DIE ZUGANGSDATEN IHRES UNTERNEHMENS IM DARK WEB ZUM KAUF ANGEBOTEN?

Digitale Anmeldeinformationen wie Benutzernamen und Kennwörter verbinden Sie und Ihre Mitarbeiter mit wichtigen Geschäftsanwendungen sowie Online-Diensten. Leider wissen das auch Kriminelle — und deshalb gehören digitale Anmeldeinformationen zu den wertvollsten Gütern, die man im Dark Web findet.

EIN DUNKLER UND GEFÄHRLICHER ORT

Das Dark Web besteht aus digitalen Communities, die sich auf einer anderen Ebene des Internets befinden. Zwar gibt es legitime Zwecke für das Dark Web, man schätzt jedoch, dass mehr als 50 % aller Websites im Dark Web für kriminelle Aktivitäten verwendet werden, einschließlich der Offenlegung und des Verkaufs digitaler Anmeldedaten. Viel zu oft wissen Unternehmen nicht, dass ihre Anmeldeinformationen gehackt und auf Dark Web verkauft wurden; und zwar solange, bis sie von den Strafverfolgungsbehörden informiert wurden — aber dann ist es zu spät.

WIE KOMMT ES DAZU?

Wenn Ihre Mitarbeiter geschäftlichen E-Mails auf Websites von Drittanbietern, wie z. B. in den unterhalb aufgeführten Kategorien, verwenden, wird Ihr Unternehmen dadurch anfälliger für Verstöße. Mit unserem Dark Web Monitoring können wir feststellen, ob für Ihr Unternehmen das Risiko besteht, dass auf diesen Websites Informationen angezeigt werden.

- HR & Lohnkonto
- E-mail-Dienste
- CRM
- Reise-Websites
- Bankwesen
- Soziale Medien

WAS KÖNNEN SIE TUN, UM IHR UNTERNEHMEN ZU SCHÜTZEN?

Mit Dark Web ID™, einer Kombination aus menschlicher und hochentwickelter Dark Web Intelligenz mit Suchfunktionen, können Sie die gefährdeten oder gestohlenen Mitarbeiter- und Kundendaten Ihres Unternehmens ermitteln, analysieren und proaktiv überwachen.

81%
der Hacker-Angriffe setzen gestohlene und/oder schwache Passwörter ein

60%
der KMU werden innerhalb von 6 Monaten nach einem Cybervorfall aus dem Geschäft ausscheiden

43%
der Cyberangriffe treffen KMU

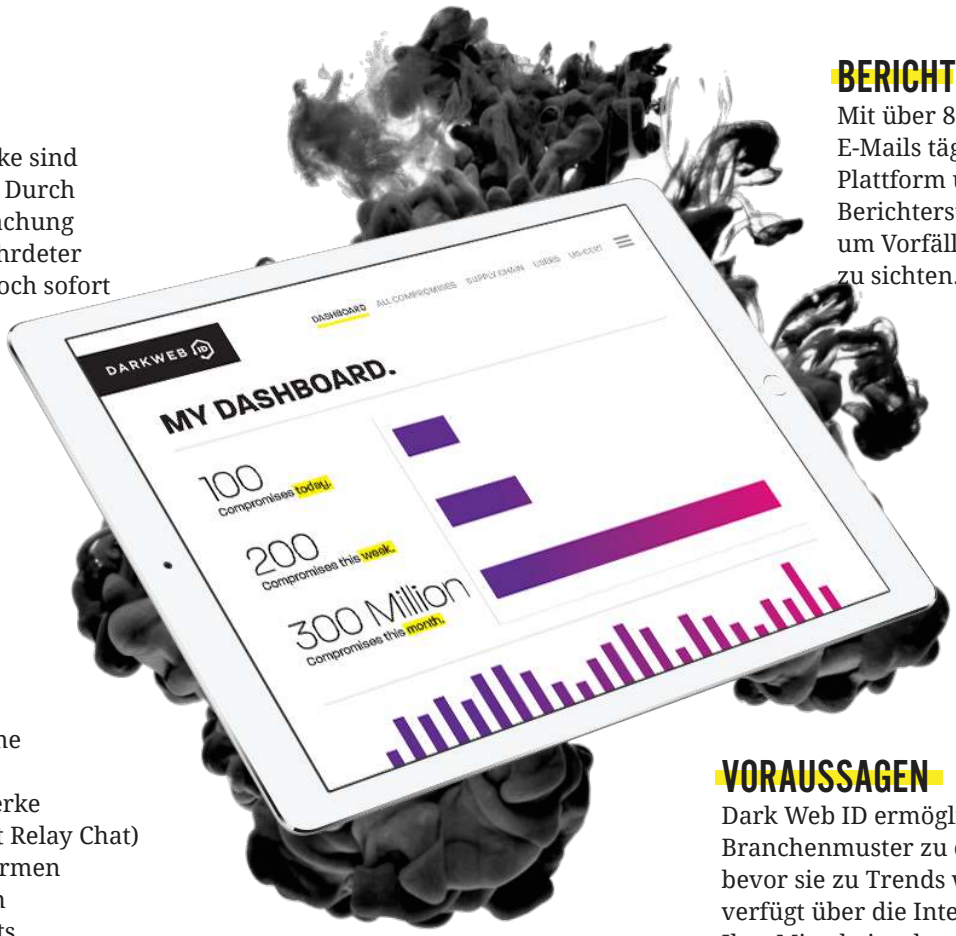
de-dsb GmbH
+49 (511) 367 392-12 | tro@de-dsb.de

DARKWEB ID

WIR BEGEBEN UNS IN DIE DUNKLE WELT, UM SIE DAVON ABZUHALTEN.

VORBEUGEN

Angriffe auf Netzwerke sind kaum zu verhindern. Durch die proaktive Überwachung gestohlener und gefährdeter Daten können Sie jedoch sofort auf eine Bedrohung reagieren, um einen schwerwiegenden Verstoß zu verhindern.



BERICHT

Mit über 80.000 gehackten E-Mails täglich bietet die Plattform umfangreiche Berichterstellungsfunktionen, um Vorfälle zu verfolgen und zu sichten.

ÜBERWACHEN 24/7/365

- Versteckte Chaträume
- Private Websites
- Peer-to-Peer-Netzwerke
- IRC-Kanäle (Internet Relay Chat)
- Social-Media-Plattformen
- Schwarzmarktseiten
- über 640.000 Botnets

VORAUSSAGEN

Dark Web ID ermöglicht es uns, Branchenmuster zu erkennen, lange bevor sie zu Trends werden, und verfügt über die Intelligenz, Sie und Ihre Mitarbeiter besser zu schützen.

WIE DARK WEB ID IHR GESCHÄFT SCHÜTZT

- Stellt eine Verbindung zu mehreren Dark Web-Diensten her, einschließlich Tor, I2P und Freenet, um nach gehackten Anmeldeinformationen zu suchen, ohne dass Sie eine direkte Verbindung zu diesen Hochrisiko-Diensten herstellen müssen.
- Bietet ein intelligentes Bewusstsein für gefährdete Anmeldeinformationen, bevor Verstöße auftreten.

WARUM ES WICHTIG IST

- Gehackte anmeldeinformationen werden für weitere kriminelle Aktivitäten verwendet.
- Mitarbeiter verwenden häufig dasselbe Kennwort für mehrere Dienste, z. B. für die Netzwerkanmeldung, soziale Medien und SaaS-Geschäftsanwendungen, wodurch der potenzielle Schaden durch eine einzige gehackte Anmeldeinformation exponentiell erhöht wird.
- Eingeschränkte Erkennbarkeit von gestohlenen Anmeldeinformationen: Über 75% der gehackten Anmeldeinformationen der betroffenen Unternehmung werden durch Dritte gemeldet, wie z. B. den Strafverfolgungsbehörden.

Kontaktieren Sie uns noch heute für einen kostenlosen und vorbereiteten Dark Web Scan!

de-dsb GmbH

DARKWEB ID

+49 (511) 367 392-12 | tro@de-dsb.de