MARKENMISSBRAUCH IM INTERNET

EINE REALE GEFAHR FÜR UND ASSET MANAGER

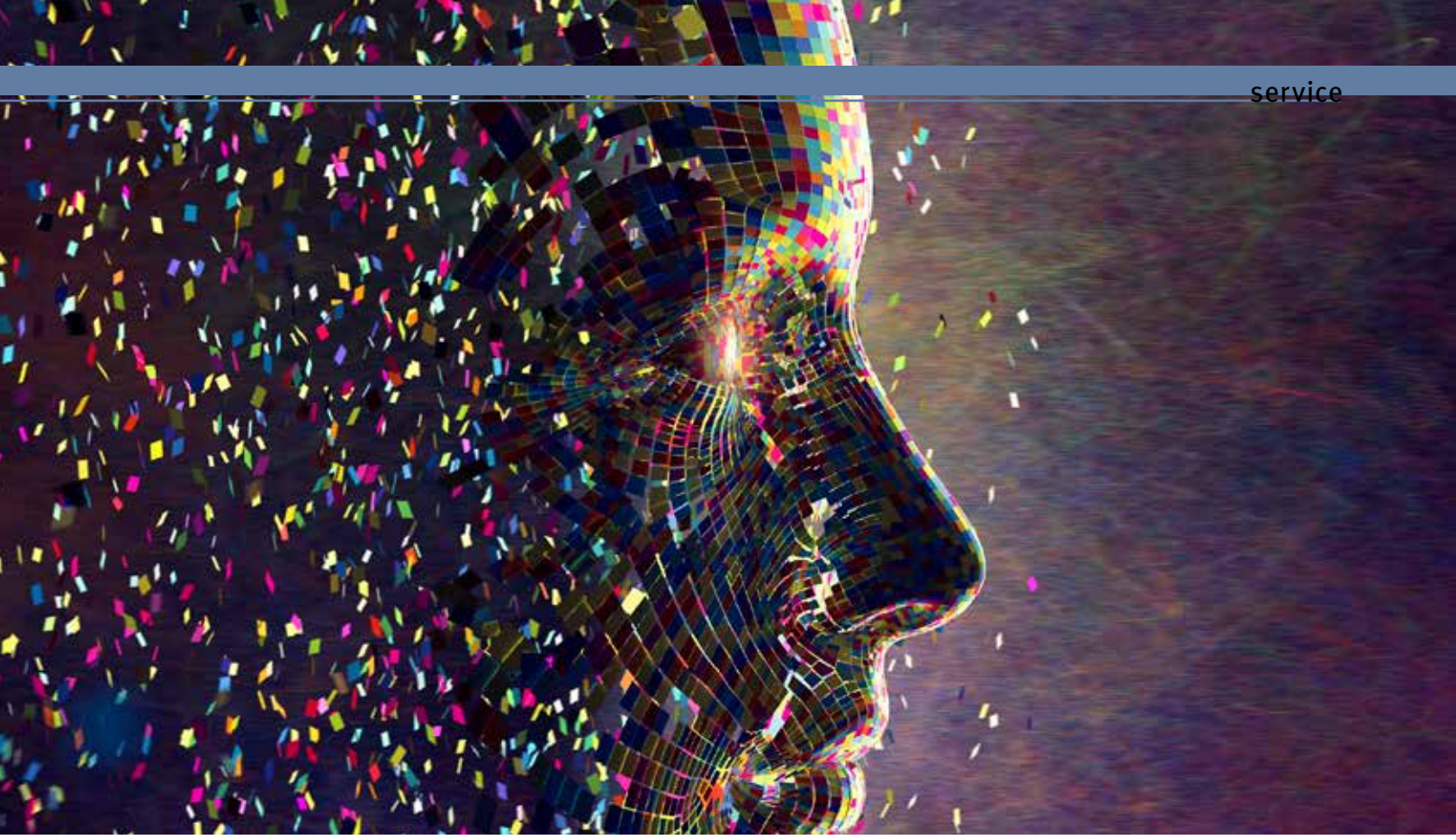
Andreas Brittner

Identitätsdiebstahl, Markenverletzungen und Online-Betrug. Die Bandbreite der Online-Kriminalität steigt – und so auch der Ideenreichtum der Betrüger. Identitäten von Vertriebsmitarbeitern in Business-Netzwerken, die Namen öffentlicher Funktionsträger aus dem Firmenimpressum oder ganze Corporate Identities inklusive identischer Bilder, Schriftarten und Logos werden zum Aufbau neuer Websites oder so genannter Fake-Profile genutzt, um potenzielle Opfer zu täuschen. Doch wie kann man seine Markenidentität schützen und welche Dinge gilt es zu beachten?

Die DZ PRIVATBANK hat seit 2020 einen Service zum Markenschutz im Einsatz und damit erste Erfahrungen gesammelt, die besonders für institutionelle Fondskunden und Kapitalanlagegesellschaften von Interesse sind. Hier ist die Bedrohungslage besonders hoch, denn die Vertriebskanäle zum privaten Anleger sind digitalisiert und die Angriffspunkte für Betrüger vielfältig.

Klassische Angriffe über Viren oder Trojaner können betroffene Unternehmen zwischenzeitlich dank immer besser werdenden Tools und Schutzmassnahmen gut im Zaum halten. Diese Bedrohungen, die über Mail-Anhänge oder Downloads von Webseiten in Unternehmensnetzwerke eindringen und sich verbreiten, werden heute dank einer Vielzahl von Schutzanwendungen und einer gestiegenen Sensibilisierung der Nutzer zum Grossteil abgehalten.

Anders sieht es in Bereichen ausserhalb der Unternehmensgrenzen aus. Ziel der Angriffe ist hier oftmals die Schwachstelle Mensch. Klassische Schutzmassnahmen zeigen häufig keine Wirkung, da Phishing-Websites, geklaute Identitäten,



FONDSINITIATOREN

Social Media Phishing oder schädliche Mobile Apps ausserhalb der eigenen Zugriffsmöglichkeiten liegen. Diese Angriffsarten werden immer komplexer und sind technisch nur schwer zu erkennen.

Phishing: Hier verschaffen sich Cyberkriminelle durch das «Abfischen» von Benutzerdaten Zugang zu Systemen eines Unternehmens. Dies geschieht häufig durch die Nutzung von Mails, welche die Leser unter einem Vorwand dazu verleiten sollen, einen Link auf eine gefälschte Webseite zu wählen und dort ihre Benutzerdaten anzugeben. Mit Zugang zu den Systemen können die Angreifer unter anderem an vertrauliche Daten gelangen und/oder schädliche Aktionen durchführen.

Social Engineering: Das Vorgehen macht sich menschliche Eigenschaften wie Vertrauen und Autorität oder Gelegenheiten zunutze, um betrügerische Handlungen auszuführen. Hierfür könnten Angreifer zum Beispiel gefälschte Profile auf Social Media-Seiten erstellen, um sich so für einen Mitarbeiter des Unternehmens auszugeben. Wenn ein Mitarbeiter beispielsweise glaubt, dass er eine Nachricht vom CEO empfängt, wird er wahrscheinlich wohlwollend auf erhaltene Anweisungen reagieren und sich eher auf den Betrug einlassen (Stichwort: CEO Scam).

Markenverletzungen oder Markenmissbrauch: In diesem Bereich nutzen Betrüger Elemente der Corporate Identity von fremden Unternehmen, um Websites oder Seiten in sozialen Medien nachzubauen. Dabei machen sie sich die Markenbekanntheit und damit das aufgebaute Vertrauen des geschädigten Unternehmens zunutze, um kriminelle Handlungen abzuleiten. Ein typisches Beispiel hierfür ist eine komplett nachgebaute Website,

welche die Kontaktdaten des Betrügers enthält und diese damit legitimieren soll. Der Betrüger könnte so etwa (potenzielle) Kunden dazu verleiten, vertrauliche Informationen preiszugeben oder unter einem Vorwand Zahlungen an ihn auszulösen. Auch das Täuschen von Konsumenten mit gefälschten Produkten fällt in diese Kategorie.

Identitätsdiebstahl: Dies ist ein Thema vor allem bei vertrauenswürdigen Persönlichkeiten. Insbesondere bei der Erstellung von betrügerischen Websites, die zwar nicht eine Unternehmensidentität kopieren, aber dennoch Nutzer zur Angabe von Daten oder zur Ausübung von Zahlungen bewegen sollen, werden für das Impressum oder als vertrieblicher Ansprechpartner geklaute Identitäten anderer Websites genutzt. Die Folgen sind je nach Betrugsart vielfältig. Typische Schäden sind Umsatz- und Reputationsverlust, sinkender Marktanteil und eine Schädigung der Geschäftsbeziehung mit den Kunden. Das Interesse, diese Schäden zu vermeiden, ist entsprechend gross. Somit steigt auch die Nachfrage nach Dienstleistungen und Systemen im Bereich des Web- und Social Media-Screenings.

Wie können sich Unternehmen gegen diese Bedrohungen schützen?

Es existieren Dienstleister, die sich darauf spezialisiert haben, die digitalen Werte eines Unternehmens ausserhalb der Unternehmens-Sicherheitsgrenzen zu schützen, zu überwachen, und Cyberkriminalität zu bekämpfen. Häufig werden hierfür Software-Lösungen auf Basis von künstlicher Intelligenz und maschinellem Lernen mit erfahrenen (menschlichen) Bedrohungsjägern kombiniert.

Zunächst wird das System mit relevanten Informationen zur Corporate Identity gefüttert, woraufhin ein Web Screening startet. Hier sind die Anzahl der Schlüsselwörter und Bilder entscheidend. Es sollte darauf geachtet werden, dass ausreichend Regionen und Sprachen berücksichtigt werden. Bei der Implementierung ist eine intensive Zusammenarbeit zwischen Servicenutzer und Serviceanbieter, aber auch zwischen internen Abteilungen notwendig. Nur wenn die gewonnenen Erkenntnisse über alle Bereiche geteilt werden, kann sich das Screening langfristig verbessern und korrekt anschlagen. In der Regel arbeiten hier IT und Marketing eng zusammen. Meist werden die erkannten Bedrohungen übersichtlich in einem Dashboard visualisiert und lassen sich daher einfach von fachkundigen Mitarbeitern nachverfolgen.

In der Praxis offerieren Anbieter verschiedene Service-Pakete als Baukasten, sodass die Dienstleistung individuell angepasst werden kann. Überwacht werden können beispielsweise auch mehrere Websites Dritter oder Social-Media-Kanäle, aber auch die Namen wichtiger Persönlichkeiten des Unternehmens wie beispielsweise die der Vorstände oder Aufsichtsräte. Auch der Bereich Mobile App Monitoring kann interessant sein. Manche Anbieter bieten auch einen Takedown-Service an, bei dem sie den Missbrauch nicht nur erkennen und klassifizieren, sondern auch die notwendigen Schritte einleiten, um die Website oder das Social Media Profil beim jeweiligen Betreiber offline nehmen zu lassen.

Aktive Massnahmen zum Markenschutz haben weitere positive Nebeneffekte bzw. Mehrwerte. Unternehmen können so erkennen, wer ihre Marke sonst im World Wide Web verwendet und wer auf Social Media mit ihrer Marke im Netz aktiv ist. Durch einen aktiven Austausch mit dem Dienstleister bleiben sie auf dem neuesten Stand hinsichtlich der aktuellen Bedrohungen.

Der wichtigste Aspekt ist aber, dass die Unternehmen durch diesen Überblick und eine schnelle Benachrichtigung bei bedrohlichen Szenarien die Möglichkeit haben, schnell Gegenmassnahmen zu veranlassen und die Gefahr zu eliminieren, bevor ein Angreifer diese aktiv ausnutzen kann.

Andreas Brittner
Gruppenleiter Medien, Kommunikation und Zusammenarbeit DZ PRIVATBANK S.A., Luxemburg.

Firmenportrait

Die DZ PRIVATBANK ist der Spezialist für Private Banking, Fondsdienstleistungen und Kredite in allen Währungen innerhalb der Genossenschaftlichen FinanzGruppe. Mit ihren Verwaltungsgesellschaften IPConcept (Luxemburg) und IPConcept (Schweiz), den Verwahrstellen in Luxemburg, Frankfurt und Zürich sowie einem umfangreichen Lagerstellennetzwerk gehört die DZ PRIVATBANK zu den führenden Anbietern von Fondsdienstleistungen im deutschsprachigen Markt. Das durch die DZ PRIVATBANK betreute Gesamtfondsvolumen beläuft sich auf aktuell 174 Milliarden EUR (Stand 31.08.2022). Gemeinsam mit der DZ BANK AG bietet die DZ PRIVATBANK über die Initiative «FONDSHAFEN» zudem Institutionellen, Vermögensverwaltern und Family Offices erstmals ein gemeinsames Asset Servicing. Investoren profitieren von langjähriger Erfahrung, Full-Service und einer persönlichen deutschsprachigen Betreuung auf Top-Niveau.