BlackBerry
Intelligent Security. Everywhere.

2021 THREAT REPORT

HIGHLIGHTS

Dieser Leitfaden stellt Ihnen die Highlights des BlackBerry® 2021 Threat Reports vor. Er basiert auf aktuellen Bedrohungsdaten von BlackBerry Kunden und anderen Sicherheitsvorfällen aus dem letzten Jahr. Sein Ziel ist eine verbesserte allgemeine Cybersicherheit. Der Report kann Ihnen dabei helfen, Mitarbeiter, Tools, Technologien und vernetzte Ressourcen effektiv und sicher einzusetzen. Er liefert Ihnen die wesentlichen Informationen, um sich gegen aktuelle Cyberbedrohungen zu wappnen. Zu jedem Thema finden Sie in diesen Highlights wichtige Sicherheitsfragen. Damit können Sie ganz einfach herausfinden, wie es in Sachen Cybersicherheit um die Vorbereitung, Prävention, Identifizierung und Reaktion in Ihrem Unternehmen steht.

CYBERSICHERHEIT, KRISEN UND CORONA

Bedrohungsakteure stellen sich schnell auf Krisen ein. Die Corona-Pandemie ist da keine Ausnahme. Als viele Mitarbeiter im letzten Frühjahr ins Homeoffice wechselten und die Unternehmen ihre Abläufe anpassten, stiegen die Cyberangriffe um 63 %[1]. Es folgte eine wahre Flut an Phishing-Kampagnen mit Corona-Bezug. Zudem entwickelten Angreifer bösartige mobile Apps, um die Unsicherheit der Menschen auszunutzen. Die Corona-Pandemie ist hierfür nur das jüngste Beispiel. Schon 2017 beim Hurrikan Harvey und 2005 beim Hurrikan Katrina gab es ähnliche Angriffe. Das Muster war immer identisch: Stört eine Katastrophe die üblichen Abläufe, wittern Angreifer ihre Chance und nutzen die Situation zu ihrem Vorteil aus.

Wichtige Sicherheitsfrage

Wie können Sie Ihr Unternehmen auf die unvermeidliche Zunahme von Cyberangriffen in Krisenzeiten vorbereiten?

1 https://www.issa.org/the-impact-of-the-covid-19-pandemic-on-cybersecurity/

RANSOMWARE-AS-A-SERVICE: ALTE BEDROHUNG, NEUE TRICKS

Die Cyberkriminellen bevorzugen mittlerweile Ransomware-as-a-Service (RaaS). Da sie von den RaaS-Anbietern mehr Support und häufigere Updates erhalten, sind ihre Kampagnen wirksamer denn je. Außerdem modifizieren sie zurzeit ihre Opfer und Methoden. Im Fokus der Angreifer stehen weniger Einzelpersonen als vielmehr große Firmen, Institutionen und ganze Branchen, wie z. B. das Gesundheitswesen. Ebenso ändert sich die Art der Erpressungsversuche. Die Angreifer drohen nicht mehr nur mit dem Löschen wichtiger Daten, sondern immer häufiger auch mit deren Veröffentlichung. Dies erhöht die Wahrscheinlichkeit, dass ein Lösegeld gezahlt wird, da das Opfer mit teuren Imageschäden rechnen muss[2].

Wichtige Sicherheitsfrage

Ist Ihr Unternehmen auf eine gezielte Ransomware-Kampagne vorbereitet und wie sieht Ihre Reaktion auf Erpressungsversuche mit exfiltrierten Daten aus?

2 https://blogs.blackberry.com/en/2020/05/threat-bulletin-ransomware-2020-state-of-play

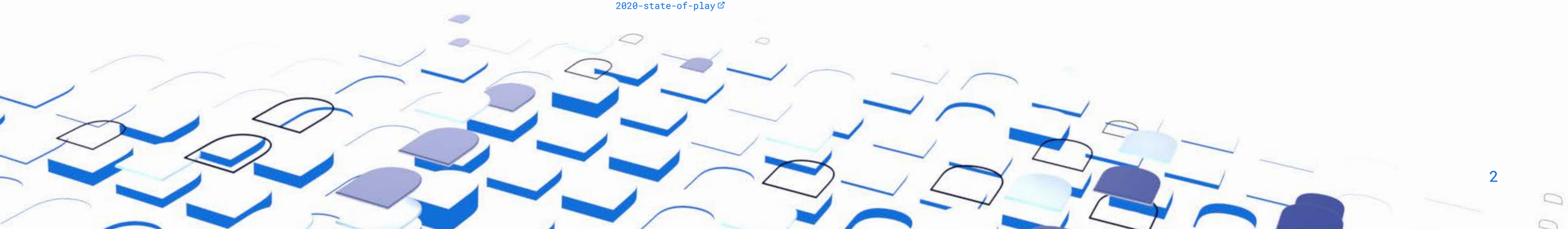
SPEAR PHISHING UND DIEBSTAHL VON ZUGANGSDATEN

Die ungewohnte und zunächst kaum geschützte Remote-Arbeit war die ideale Gelegenheit für Cyberkriminelle, um Phishing-Angriffe mit Corona-Bezug zu starten. Nach Angaben der Anti-Phishing Working Group ist die Zahl der Phishing-Kampagnen seit März 2020 signifikant gestiegen[3]. Besonders häufig waren Software-as-a-Service (SaaS)-Anwendungen und Webmail von Phishing-Angriffen betroffen. BlackBerry Experten beobachteten auch den vermehrten Einsatz von trojanisierten Anwendungen, um 0auth-Zugriffstoken zu stehlen. Diese Kampagnenart, auch „Consent Phishing“ genannt, ermöglicht es Angreifern, die Multi-Faktor-Authentifizierung (MFA) zu umgehen.

Wichtige Sicherheitsfrage

Welche Maßnahmen können Sie, Ihre Mitarbeiter und Ihr Unternehmen ergreifen, um nicht Opfer raffinierter Phishing-Angriffe zu werden?

3 https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf



KRYPTOJACKING

Kryptojacking bezeichnet die unbefugte Nutzung eines Computers zum Schürfen von Kryptowährung. Angreifer nutzen Kryptojacking, um illegal an Kryptowährung zu gelangen und sich die Schürfkosten zu sparen. Aus diesem Grund suchen sich Kryptojacker auch gern leistungsstarke Server in Unternehmensumgebungen aus. Bedrohungsakteuren stehen mehrere Wege offen, um Geräte mit Krypotojacking-Malware zu infizieren. Zwei gängige Angriffsvektoren sind bösartige Links oder in Webseiten eingebettete Kryptomining-Skripte. Ist ein Gerät erst einmal infiziert, kann es der Angreifer direkt und meist unbemerkt zum Schürfen nutzen.

Wichtige Sicherheitsfrage

Wie erkennt und identifiziert Ihr Unternehmen Kryptojacking-Angriffe, die häufig längere Zeit unbemerkt im Hintergrund ablaufen?

HERKÖMMLICHE BEDROHUNGEN

Nicht alle Cyberangriffe sind hochmodern oder werden von hochbegabten Akteuren durchgeführt. Cyberangriffe sind mittlerweile zu einem Massenprodukt geworden, bei dem die ständige Nachfrage die Entwicklung einfacher Standardangebote vorantreibt. 2020 nutzten viele Angreifer vorgefertigte Bedrohungstools und Threat-Dienste wie Exploit Kits, Malspam-Kampagnen, Software zur Nachahmung von Bedrohungen sowie Mimikatz. Zur Informationssammlung, zum Domain-Mapping und für Lateral Movement innerhalb einer Umgebung setzten die Angreifer vor allem Tools wie Adfind und Sharphound ein.

Wichtige Sicherheitsfrage

Wie erkennt Ihr Unternehmen herkömmliche Bedrohungen von böswilligen Akteuren oder Gruppen und wie reagieren Sie darauf?

MOBILE SICHERHEIT

Bei Overlay-Angriffen geht es vor allem um Spionage und das Erbeuten wertvoller, persönliche Daten. Die Angreifer nutzen dabei die Erwartungen der Anwender und anfällige Smartphone-Overlay-Dienste aus. Der Ansatz ist denkbar einfach: Die überlagernde App startet exakt dann, wenn der Anwender auf seine scheinbar legitime App zugreift. Die Anwender schöpfen keinen Verdacht, auch wenn sie unvermittelt zur Eingabe sensibler Daten aufgefordert werden. Bei Overlay-Angriffen kommen vor allem Malware-Familien wie Anubis, Ginp, Cerberus, EventBot und Marcher zum Einsatz, die es auf Bank- und Zugangsdaten abgesehen haben.

Wichtige Sicherheitsfrage

Wie schützen Sie Smartphones, die auf geschäftliche und persönliche Daten zugreifen, vor Overlay-Angriffen?

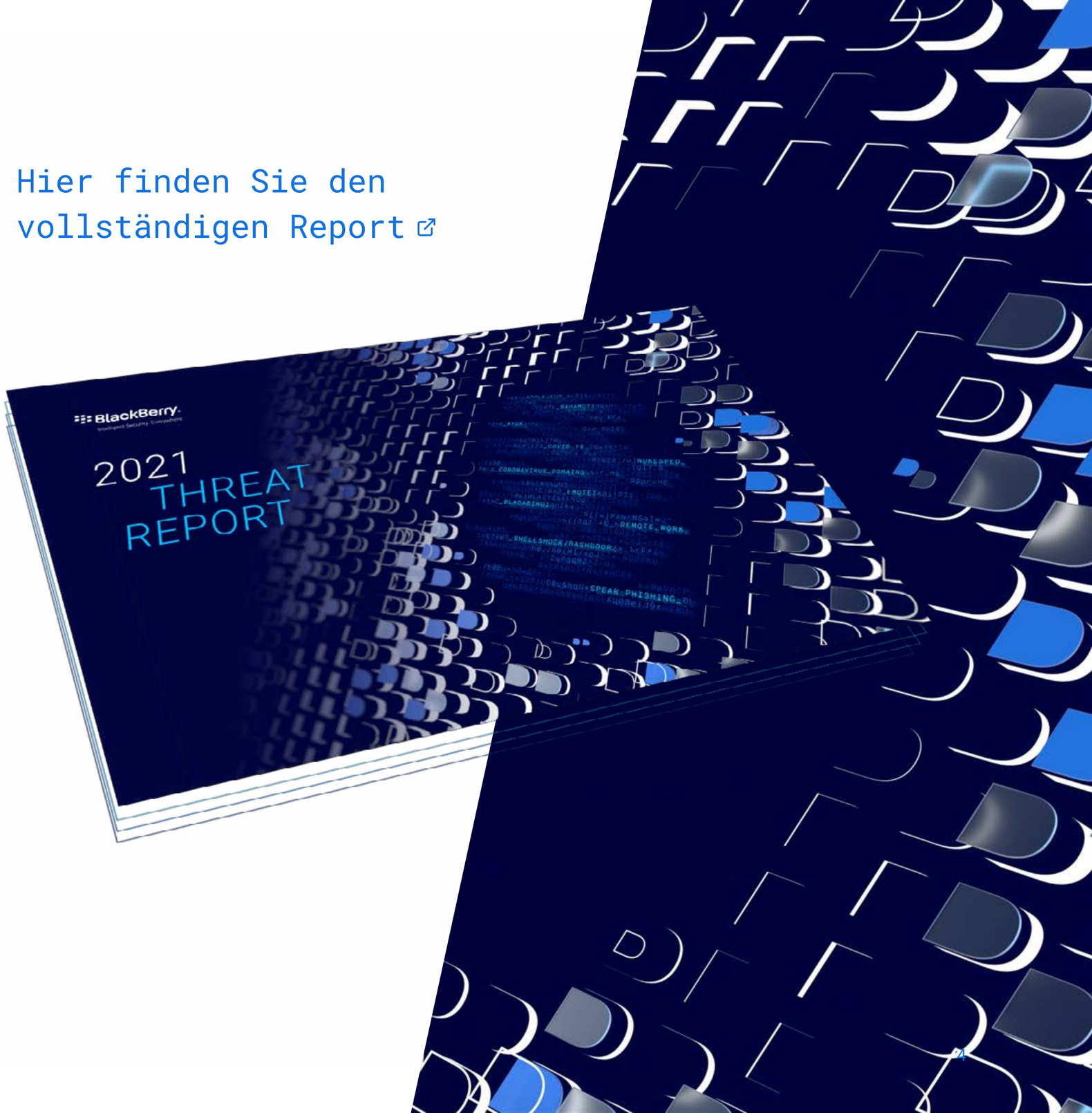
TÄUSCHEND ECHTE DEEPFAKES

2020 wurden Deepfake-Attacken erstmals auch am Arbeitsplatz entdeckt. Zu den ersten Opfern gehörte ein hoher Beamter, der zu einer Überweisung verleitet wurde, nachdem er einen vermeintlichen Anruf seines CEOs erhalten hatte. Dessen Stimme war mithilfe von KI täuschend echt imitiert worden[4]. Im letzten Frühjahr machte auch ein Deepfake-Video der belgischen Premierministerin die Runde, in dem sie die Ursache für die Pandemie mit Umweltschäden in Verbindung zu bringen schien[5]. Es braucht kein tiefgreifendes Fachwissen oder ein gewaltiges Kapital, um Deepfake-Audios und -Videos zu erstellen. Sicherheitsforscher machten mehrere Untergrundforen ausfindig, in denen Deepfake-Dienste verkauft werden und Akteure nach Möglichkeiten suchen, diese Technologie zu monetarisieren. Deepfakes haben sich mittlerweile zu treuen Begleitern von Desinformationskampagnen entwickelt[6].

Wichtige Sicherheitsfrage

Wie schützen und verifizieren Sie die Identität Ihrer Führungskräfte und welche Maßnahmen ergreifen Sie zukünftig, um Ihr Unternehmen vor dieser wachsenden Bedrohung zu schützen?

Hier finden Sie den vollständigen Report



4 https://www.bbc.com/news/technology-48908736

5 https://www.brusselstimes.com/news/belgium-all-news/politics/106320/xr-belgium-posts-deepfake-of-belgian-premier-linking-covid-19-with-climate-crisis/

6 https://cpb-us-e1.wpmucdn.com/sites.uw.edu/dist/6/4560/files/2020/10/CIP_Deepfakes_Report_Extended.pdf

BlackBerry

Intelligent Security. Everywhere.