proofpoint.

Sie haben BEC!

Die 10 größten, gefährlichsten und dreistesten BEC-Betrugsversuche von 2020 und 2019

proofpoint.com/de

EINFÜHRUNG

Es ist schwieriger als es aussieht, BEC-E-Mails zuverlässig als solche zu entlarven. Der Grund: BEC-Angriffe (Business Email Compromise, auch unter den Begriffen Chefmasche oder CEO-Betrug bekannt) nutzen das menschliche Verhalten aus. Dies ist eine Aufstellung der bekanntesten (und niederträchtigsten) BEC- und EAC-Angriffe der letzten 12 Monate.

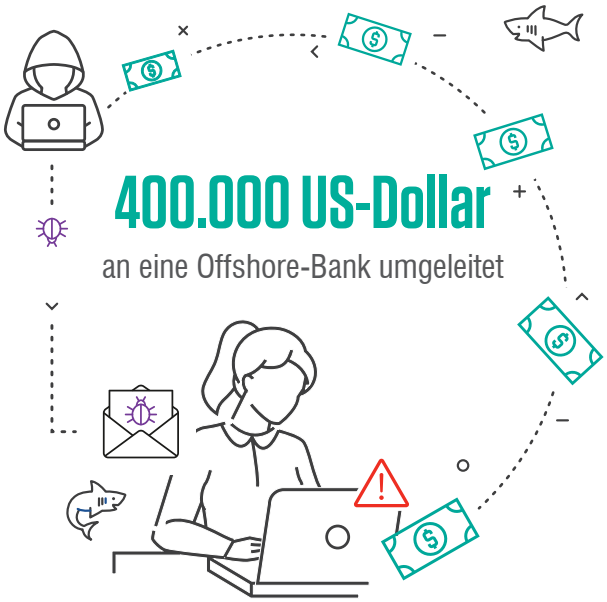
Die Anfrage stammt von der richtigen Person und auch der Inhalt der Anfrage – etwa eine Banküberweisung vorzunehmen oder Auskunft zu vertraulichen Mitarbeiterdaten zu geben – gehört durchaus zum Tagesgeschäft des jeweiligen Mitarbeiters. Indem der Absender dieser Anfragen seine Identität fälscht, gelingt es ihm, den Ansprechpartner zu überlisten. Ein teurer Irrtum.

Das Problem dabei: Es ist nicht immer einfach, authentische E-Mails und betrügerische Nachrichten zu unterscheiden.

BEC-Angriffe nutzen just die für Menschen typischen Eigenschaften aus, die eine funktionierende Gesellschaft sowie reibungslose Abläufe in Unternehmen erst ermöglichen. Die BEC-Betrüger setzen auf menschliche Psychologie und beziehen sich auf reguläre Geschäftsprozesse, um Ihre Anwender zu verleiten, Gelder zu überweisen, Überweisungen und Zahlungen umzuleiten oder vertrauliche Informationen zu versenden.

Die Kompromittierung von E-Mail-Konten (Email Account Compromise, EAC) ist eng mit BEC verwandt. Doch anstatt lediglich mithilfe eines Doppelgänger-Kontos eine Person zu imitieren, der ein Anwender vertraut, kapern EAC-Angreifer das tatsächliche Konto der vertrauenswürdigen Person.

Es überrascht nicht, dass die Opfer von BEC-Betrugsversuchen bereits Milliarden US-Dollar verloren haben – mit steigender Tendenz. Im Folgenden stellen wir einige der größten, gefährlichsten und dreistesten Betrugsversuche der letzten Monate vor.



1. Barbara Corcoran von „Shark Tank“

ABC-TV beschreibt die Stars der erfolgreichen Sendung „Shark Tank“ (vergleichbar mit der hierzulande beliebten „Höhle der Löwen“) als „knallharte Selfmade-Multimillionäre und Top-Milliardäre“. Das heißt jedoch nicht, dass sie nicht hereingelegt werden können.

Barbara Corcoran gehört zu den Juroren der Sendung, die entscheiden, ob die Vorhaben unterschiedlichster Unternehmer eine Finanzierung erhalten sollten. Im Februar war sie es jedoch, die durch einen BEC-Betrug fast 400.000 US-Dollar verlor.

Corcoran, die ihr Vermögen als Immobilienmaklerin gemacht hat, gab Ende Februar 2020 bekannt, dass ihr Buchhalter das Geld an eine Person überwiesen hatte, die sich als Corcorans Assistent ausgab. Von der Summe sollte die Renovierung einer Immobilie bezahlt werden. Nachdem die Überweisung erfolgt war, fiel Corcoran auf, dass die E-Mail-Adresse des angeblichen Assistenten falsch war: Ein Buchstabe stimmte nicht.

„Ich hatte keinen Grund misstrauisch zu sein, da ich viel im Immobilienbereich investiere“, erklärte Corcoran der Zeitschrift *People*.[1]

Corcorans IT-Mitarbeiter konnten den Angriff später zu einer chinesischen IP-Adresse zurückverfolgen.

Mittlerweile hat Corcoran das Geld zurück erhalten. Auf dem Weg zum Konto des Betrügers in China hatte die Überweisung den Weg über eine Bank in Deutschland genommen.[2] Corcorans Bank forderte die deutsche Bank auf, das Geld einzufrieren, was ihr die nötige Zeit verschaffte, den Betrug nachzuweisen.

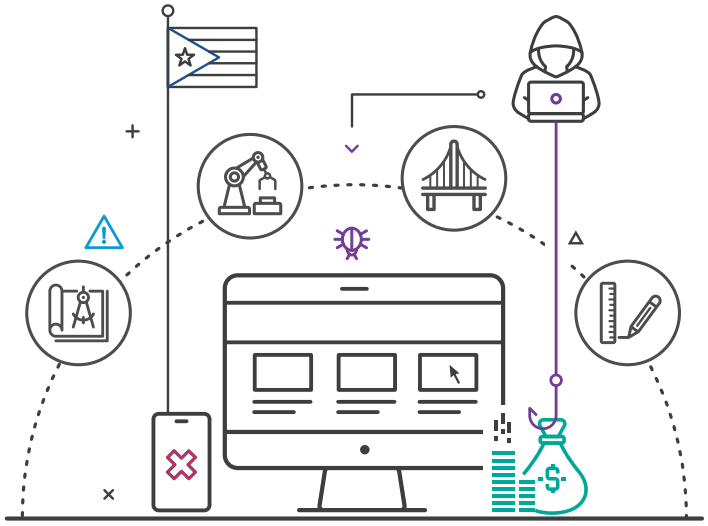
An diesem Fall zeigt sich eines der zentralen Merkmale von BEC-Betrugsversuchen – die Routinemäßigkeit der E-Mails, die sie unverdächtig macht.

[1] Robyn Merrett (People): „Shark Tank‘s Barbara Corcoran Gets Back $388K Stolen in Phishing Scam: ‚I‘m Thrilled!‘“ (Barbara Corcoran von Shark Tank erhält nach Phishing-Betrug gestohlene 388.000 USD zurück: „Ich bin begeistert!“), März 2020.

[2] ebd.

2. Puerto Rico

Puerto Rico wurde in letzter Zeit mehrfach heftig gebeutelt. Das Land wurde unter anderem von Hurrikans, einer Schuldenkrise sowie einer Rezession heimgesucht – und nun auch von BEC-Angriffen.



4 Mio. US-Dollar

bei drei separaten BEC-Angriffen geraubt

Im Januar büßte Puerto Rico im Zuge dreier unterschiedlicher BEC-Angriffe auf Behörden mehr als 4 Millionen US-Dollar ein.[3]

Am Anfang des Betruges stand die Kompromittierung des Computers eines Mitarbeiters der Finanzabteilung beim Federal Employees Retirement System (Bundesrentenkasse) von Puerto Rico einen Monat zuvor. Mit dem Konto des Mitarbeiters konnte der Angreifer E-Mails an dessen Kollegen in anderen Behörden senden. Dabei wurden die Empfänger aufgefordert, die Bankkontonummer für Überweisungen zu ändern.

Technisch gesehen ist dies ein EAC-Angriff (Email Account Compromise), da der Angreifer nicht eine nur scheinbar legitime E-Mail-Adresse verwendet, sondern ein reales Konto missbraucht.

Der größte Diebstahl fand bei der Industrial Development Company von Puerto Rico statt, einem staatlichen Unternehmen, das die wirtschaftliche Entwicklung der Insel vorantreibt. Dabei wurden 2,6 Millionen US-Dollar an staatlichen Geldern geraubt.[4] Die Puerto Rican Tourism Company wurde um 1,5 Millionen US-Dollar erleichtert, während die Commerce and Export Company 63.000 US-Dollar verlor.

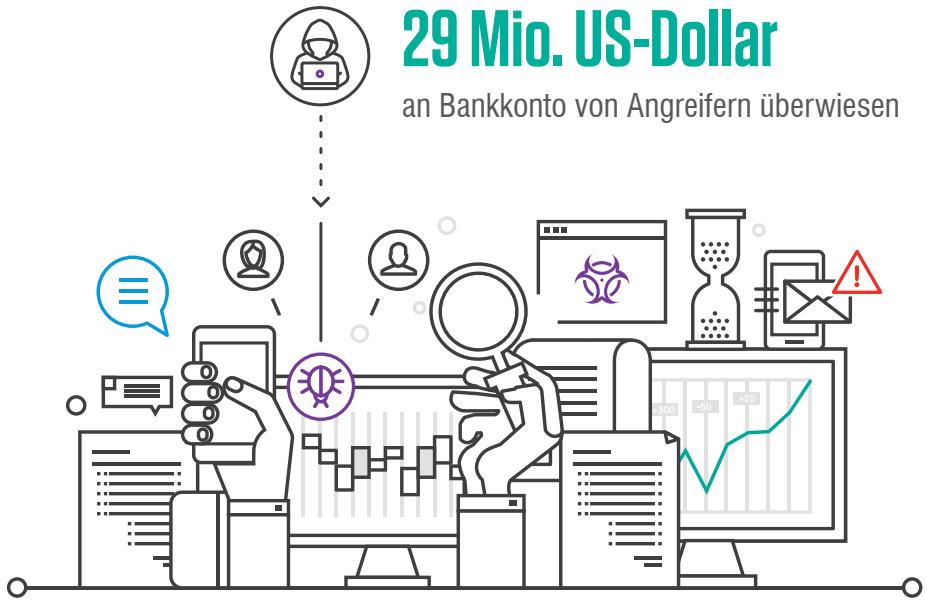
Wie bei den meisten BEC-Angriffen zeigte sich auch hier, dass die Schwachstelle bei den Menschen lag.

„Der Staat versagte nicht auf technischer Ebene, sondern bei seinen Verfahren“, betont José Quiñones, Präsident der gemeinnützigen Cybersicherheitsorganisation Obsidis Consortia in Puerto Rico, gegenüber Associated Press.[5]

[3] Dánica Coto (Associated Press): „3 employees suspended in $4M Puerto Rico online scam“ (3 Angestellte in Puerto Rico nach Online-Betrug mit 4 Mio. USD Schaden suspendiert), Februar 2020.

[4] Dánica Coto (Associated Press): „Official: Puerto Rico govt loses $2.6M in phishing scam“ (Regierung von Puerto Rico verliert 2,6 Mio. USD durch Phishing-Betrug), Februar 2020.

[3] Dánica Coto (Associated Press): „3 employees suspended in $4M Puerto Rico online scam“ (3 Angestellte in Puerto Rico nach Online-Betrug mit 4 Mio. USD Schaden suspendiert), Februar 2020.



3. Nikkei

Der japanische Mediengigant Nikkei zählt sicher nicht zu den typischen Opfern von Finanzbetrug.

Nikkei gehört zu Japans größten Medienkonglomeraten, besitzt die in London ansässige *Financial Times* und ist Namensgeber des Aktienindex an der Tokioter Börse.

Seine schiere Größe und Finanzstärke machen den Giganten zu einem attraktiven Ziel für Betrüger. Im September 2019 überwies ein Mitarbeiter des amerikanischen Ablegers Nikkei America die Summe von 29 Millionen US-Dollar und folgte dabei Anweisungen, die er per E-Mail scheinbar von einer Führungskraft des Mutterunternehmens erhalten hatte.

Tatsächlich stammte die E-Mail jedoch von einem Betrüger, wobei einige Berichte darauf hindeuten, dass der Angreifer das Konto des Managers gekapert haben könnte[6], sodass wir es hier möglicherweise mit einem EAC-Angriff zu tun haben. Das Medienunternehmen und die Behörden haben nur wenige Details bekanntgegeben.

Unternehmensvertreter erklärten, der Mediengigant würde versuchen, das Geld zurückzuholen. Über den Erfolg dieser Bemühungen ist jedoch nichts bekannt.[7]

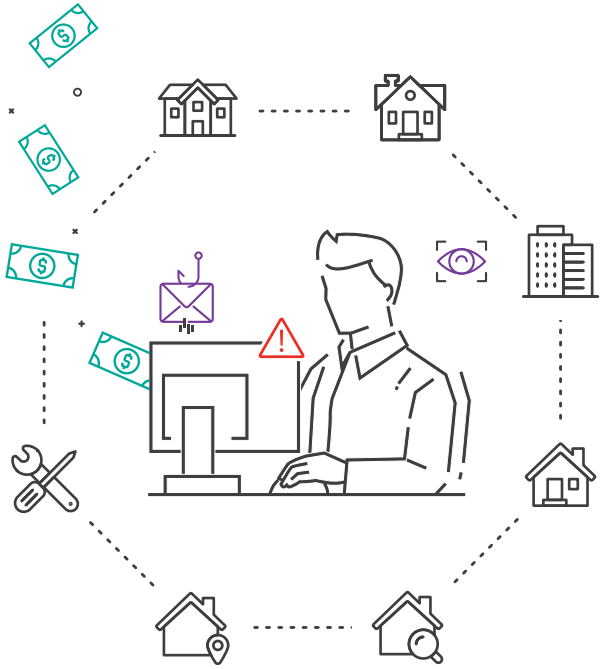
[6] Lindsey O'Donnell (ThreatPost): „BEC Scam Costs Media Giant Nikkei $29 Million" (BEC-Betrug kostet Mediengigant Nikkei 29 Mio. USD), November 2019.

[7] Nikkei: „Matter concerning transfer of funds at Nikkei Inc.'s US subsidiary" (Vorfall mit Überweisung von Geldern beim US-Ableger von Nikkei Inc.), Oktober 2019.

4. Red Kite Community Housing

1,2 Mio. US-Dollar

von Wohltätigkeitsorganisation gestohlen



Wer sich in der britischen Stadt High Wycombe unweit von London keine Unterkunft leisten kann, findet Hilfe bei Red Kite Community Housing. Die gemeinnützige Organisation besitzt und verwaltet mehr als 6.500 Häuser im Bezirk Wycombe, die sie an Geringverdiener zu Preisen unterhalb des Marktwertes vermietet.

Im August 2019 musste Red Kite jedoch bei einem BEC-Angriff einen herben finanziellen Verlust von 932.000 Britischen Pfund (1,04 Millionen Euro) verkraften.

Laut Medienberichten konnten die Cyberangreifer als einer der Lieferanten von Red Kite auftreten, indem sie eine Doppelgänger-Domäne registrierten. Mithilfe der gefälschten Domäne, die der des echten Vertragspartner sehr ähnlich sah, verleiteten die Angreifer den Empfänger zum Überweisen der Summe an das Bankkonto der Angreifer. Der E-Mail-Text enthielt, um zusätzliche Legitimität zu suggerieren, einen erfundenen Nachrichtenverlauf, der wie eine längere Konversation zwischen Red Kite-Führungskräften und dem Vertragspartner wirkte.[8]

Die Sicherheit bei Red Kite wird unter anderem durch Zwei-Faktor-Authentifizierung gewährleistet, die Änderungen an Überweisungen und Konten verifiziert, wie ein Pressesprecher von Red Kite gegenüber der IT-News-Website *Digit* erklärte.[9]

Red Kite betonte, dass die eigenen Systeme zu keinem Zeitpunkt kompromittiert waren, sondern ein Mitarbeiter die Schwachstelle war. Dieser hatte sich von der E-Mail täuschen lassen und war nicht dem normalen Verfahrensweg gefolgt.

„Dieses Einfallstor haben wir mit internen Schulungen und veränderten Prozessen geschlossen“, gab die Gesellschaft bekannt.[10]

Red Kite meldete die Kompromittierung den Mitgliedern (die nicht mit den Kosten durch den Diebstahl belastet wurden), der örtlichen Polizei, einem externen Cyberforensikunternehmen sowie einer regionalen Behörde für die sozialen Wohnungsbau.[11]

Die gemeinnützige Organisation hat seither die Sicherheitslage verbessert, einen Audit seiner Prozesse und Systeme durchgeführt sowie zusätzliche Sicherheitsmaßnahmen wie Mitarbeiterschulungen implementiert.

[8] Lucie Heath *(Inside Housing)*: „Housing association defrauded of nearly £1m after falling victim to cyber scam“ (Wohnungsbaugesellschaft mit Cyberbetrug um fast 1 Mio. GBP geprellt), Januar 2020.

[9] David Paul, *(Digit)*: „British Charity Loses almost £1m in Domain Spoofing Scam“ (Britische gemeinnützige Organisation verliert fast 1 Mio. GBP durch Domain-Spoofing-Betrug), Februar 2020.

[10] Red Kite Community Housing: https://redkitehousing.org.uk/

[11] Tara Seals *(ThreatPost.com)*: „Community Housing Nonprofit Hit with $1.2M Loss in BEC Scam“ (Gemeinnützige Wohnungsbaugesellschaft verliert 1,2 Mio. USD durch BEC-Betrug), Februar 2020.

5. Mitglieder jüdischer Synagogen

53 %

der von Secure Community Network Befragten wurden mit BEC-Betrugsversuchen angegriffen

Alle BEC-Betrugsversuche haben gemeinsam, dass der Empfänger der E-Mail den scheinbaren Absender kennt, ihn respektiert und ihm vertraut. Meist sind das Kollegen, Geschäftspartner oder Vorgesetzte. Für viele gläubige Juden in den USA zählt auch der Rabbiner ihrer Synagoge zu den vertrauenswürdigen Autoritätspersonen.

In den Regionen Detroit, San Francisco Bay Area, Idaho, Tennessee sowie weiteren Gemeinden in den USA setzten unbekannte Angreifer auf eine neue Variante des seit langem erfolgreichen Gutscheinkarten-Betrugs. Dabei gaben sie sich als der örtliche Rabbiner aus und baten die Empfänger – meist im Rahmen einer angeblichen Spendenaktion – Gutscheinkarten zu kaufen.

Drei Mitglieder einer Synagoge in Virginia fielen darauf herein und kauften Gutscheinkarten im Wert von insgesamt 2.500 US-Dollar. Bislang konnte lediglich zwei der drei Opfer die Gutscheinkarten stornieren und ihr Geld zurückholen.

In Idaho hätte eine Frau beinahe 400 US-Dollar in Gutscheinkarten an die Betrüger verloren. Einem aufmerksamen Kassierer fiel auf, wie sie Fotos der Karten sowie der Kontonummer und PIN machte, die sie an die E-Mail-Adresse des falschen Rabbiners senden wollte, woraufhin er noch rechtzeitig einschritt.[12]

„Diese Betrugsmethode funktioniert deshalb so zuverlässig, weil die Mitglieder der Gemeinde ihrem Geistlichen vertrauen“, so Rabbinerin Debra Newman Kamin, Präsidentin der Rabbinical Assembly, einer konservativen Vereinigung von Rabbinern.[13]

Während das FBI und die Federal Trade Commission (Bundeshandelskommission, FTC) allgemeine Warnungen zu Gutscheinkarten-Betrug an die Öffentlichkeit richteten, veranlasste die Welle von Angriffen auf jüdische Gemeinden das Secure Community Network (SCN) zu einer Reaktion.

Diese Initiative für Heimatsicherheit der North American Jewish Community meldete, dass im Jahr 2019 53 % der befragten Organisationen – Unternehmen aller Art, aber auch örtliche Behörden und religiöse Gruppen – Cyberangriffe meldeten. Im Jahr zuvor waren es noch 38 %.

[12] Ari Feldman *(Forward)*: „‘Rabbi‘ gift card scam spurred congregants to spend thousands“ (Rabbiner-Gutscheinkarten-Betrug veranlasst Gemeindemitglieder, tausende US-Dollar zu spenden), Februar 2020.

[13] Rabbiner Jason Miller *(The Jewish News)*: „Email Spoofing Scam Targets Rabbis and Congregants in Metro Detroit“ (E-Mail-Betrugsversuche richten sich gegen Rabbiner und Gemeindemitglieder im Großraum Detroit), Februar 2020.

6. Unabhängiger Schulbezirk Manor

Eine Welle von Cyberangriffen in den USA richtete sich in den letzten Monaten gegen kleine Städte, lokale Ämter und Schulbezirke. Dabei könnten die Angreifer davon ausgehen, dass kleinere und teils unterfinanzierte lokale Behörden weniger Geld für Cybersicherheit zur Verfügung haben als größere Behörden oder der private Sektor. In vielen Fällen liegen sie damit richtig.

Das ist jedoch nur ein Teil der Wahrheit. Bei kleinen ebenso wie bei großen Unternehmen sind üblicherweise die Mitarbeiter das schwächste Glied in der Sicherheitskette.

2,3 Mio. US-Dollar

bei einem einzigen BEC-Angriff gestohlen

Ein typisches Beispiel ist der unabhängige Schulbezirk Manor (Manor Independent School District) unweit von Austin, Texas. Der Bezirk mit 9.600 Schülern wurde im November 2019 bei einem BEC-E-Mail-Angriff um 2,3 Millionen US-Dollar betrogen.

Beginnend mit November 2019 kontaktierten die Betrüger über mehrere Monate hinweg verschiedene Bezirksmitarbeiter und ließen die Zahlungsdaten eines Lieferanten ändern. Nur ein Mitarbeiter fiel auf die E-Mail herein, doch der Schaden war enorm. Die Betrüger konnten drei separate Überweisungen anstoßen, bevor jemand stutzig wurde.[14]

Der Schulbezirk hofft, 800.000 US-Dollar aus einer Versicherung zurückzuerhalten und müsste dann einen Nettoverlust von 1,5 Millionen US-Dollar verkraften.

[14] Drew Knight, Luis de Len, KVUE-TV: „Manor ISD loses $2.3 million in phishing scam; police and FBI investigating“ (Manor ISD verliert 2,3 Mio. USD bei Phishing-Betrug; Polizei und FBI ermitteln), Januar 2020.

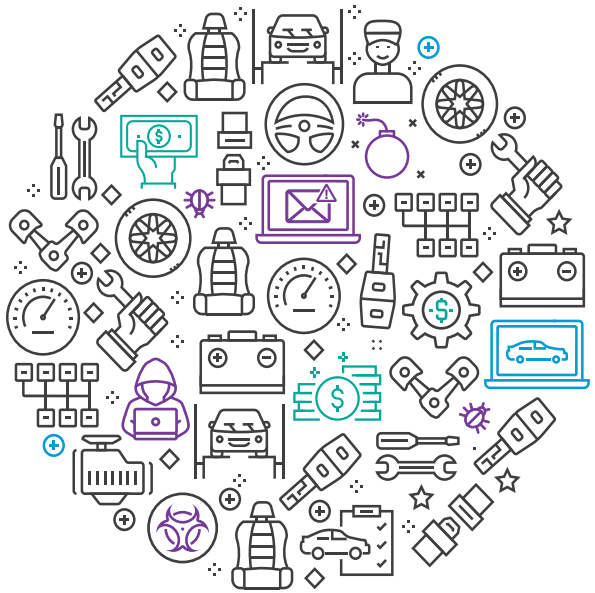
7. Toyota Boshoku

BEC-Angreifer attackieren kleine ebenso wie große Unternehmen. Zu den größten Opfern – mit einer der größten Schadenssummen – der letzten Monate gehört Toyota Boshoku. Das Tochterunternehmen von Toyota, das Autositze und weitere Komponenten für die Inneneinrichtung produziert, wurde im August 2019 um 37 Millionen US-Dollar betrogen.

Laut Medienberichten handelte es sich bei dem Angriff um klassisches BEC. Jemand gab sich als Geschäftspartner aus, sendete E-Mails an Mitarbeiter in der Finanz- und Rechnungsabteilung und forderte Zahlungen an das Bankkonto des Angreifers an.[15]

Das Unternehmen gab bekannt, dass es schnell auf den Betrug aufmerksam wurde, ihn den Behörden meldete und daran arbeitet, das Geld zurückzubekommen.

Der Angriff mit einem Schaden von 37 Millionen US-Dollar verdeutlicht, wie Social Engineering selbst die am besten finanzierten Cyberschutzmaßnahmen unterlaufen können, da sich diese Taktik gegen Menschen und nicht die Infrastruktur richtet.

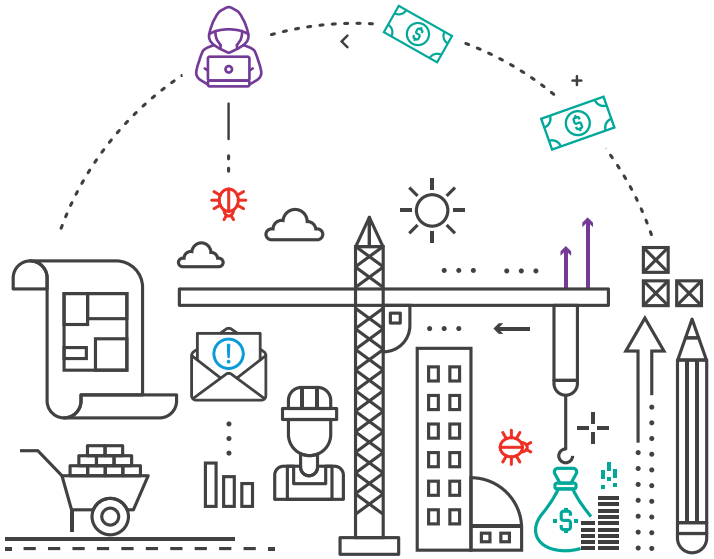


37 Mio. US-Dollar

beim größten BEC-Angriff gestohlen

[15] Nicole Lindsey *(CPO Magazine)*: „Toyota Subsidiary Loses $37 Million Due to BEC“ (Toyota-Tochterunternehmen verliert 37 Mio. USD durch BEC), September 2019.

8. Cabarrus County (North Carolina, USA)



2,5 Mio. US-Dollar

mithilfe gefälschter Unterlagen gestohlen

Cabarrus County in North Carolina (USA) gab Ende 2018 stolz Pläne bekannt, für 2,5 Millionen US-Dollar die West Cabarrus High School zu bauen. Anscheinend war dies den BEC-Betrügern auch nicht entgangen.

Während der Bauphase im November erhielt der Schulbezirk eine E-Mail, die scheinbar vom Generalunternehmer stammte, der den Bau der Schule übernahm. Sie enthielt neue EFT-Kontodetails (Electronic Funds Transfer) zur Bezahlung des Unternehmers sowie unterzeichnete Autorisierungen und weitere Dokumentation. Einige wenige Wochen später überwies der Bezirk wie angewiesen eine Summe auf das neue Konto.

Bis Januar fiel niemandem etwas auf. Erst dann erhielten die Verantwortlichen eine Nachricht vom Auftragnehmer über die fehlende Bezahlung.

Die Schulbeamten entdeckten schnell, dass alles in der E-Mail – Kontoangaben, Dokumente und Unterschriften – gefälscht war. Der Bezirk konnte 776.518,40 US-Dollar zurückholen, die übrigen 1.728.082,60 US-Dollar waren verloren, umgeleitet und gewaschen über ein ganzes Netzwerk verschiedenster Bankkonten.[16]

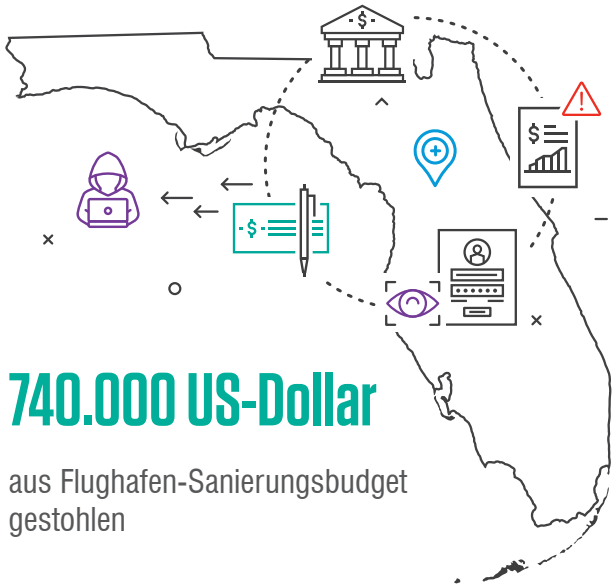
Um die Bauarbeiten nicht zu unterbrechen, musste der Beauftragtenrat (Board of Commissioners) von Cabarrus County die fehlenden Gelder aus einem Sonderfonds für „außergewöhnliche Situationen“ bereitstellen.[17]

Laut der neuesten Informationslage aus dem County werden die Ermittlungen fortgesetzt.

[16] Ionut Arghire (SecurityWeek): „Scammers Grab $2.5 Million From North Carolina County in BEC Scam“ (Betrüger erbeuten mit BEC 2,5 Mio. USD von County in North Carolina), August 2019.

[17] Cabarrus County: „Cabarrus County Government targeted in social engineering scam“ (Verwaltung von Cabarrus County mit Social-Engineering-Betrug angegriffen), August 2019.

9. Ocala (Florida, USA)



740.000 US-Dollar

aus Flughafen-Sanierungsbudget gestohlen

Beobachter der Cybersicherheitslage können den kleinen Ort Ocala in Florida mit seinen kaum 60.000 Einwohnern in die Liste der Kleinstädte aufnehmen, die Opfer vonCyberkriminellen wurden.

Im September 2019 verlor die Stadt mehr als 740.000 US-Dollar bei einem BEC-Angriff, der ein nahegelegenes, im Bau befindliches Flughafen-Terminal zum Ziel hatte.

Ebenso wie bei anderen BEC-Angriffen stand am Anfang eine E-Mail an den leitenden Bilanzbuchhalter der Stadt, die scheinbar vom Buchhalter der ausführenden Baufirma stammte.

Die Nachricht enthielt ein behördliches Formular zur Änderung der Bankdaten des Unternehmens, darin enthalten die Kontonummer und Bankleitzahl des neuen Kontos sowie – um die Täuschung noch glaubwürdiger zu machen – den Scan eines annullierten Schecks, der auf eben dieses Konto ausgestellt war.[18]

Nachdem die echte Baufirma am 17. Oktober eine Rechnung stellte, zahlte die Stadt am nächsten Tag – an das Konto des Betrügers. Einige Tage später fragte die Baufirma nach, warum sie noch kein Geld erhalten hatte.[19]

Der städtische Mitarbeiter, der die Überweisung genehmigt hatte, kündigte kurz nach Bekanntwerden des Betrugs.[20] Allerdings hätte beinahe jeder auf diese Täuschung hereinfallen können.

Die E-Mail missbrauchte den Namen eines früheren Mitarbeiters des Bauunternehmens und nutzte eine Doppelgänger-Domäne, die sich von der echten Domäne lediglich durch einen einzigen Buchstaben unterschied – ein zusätzliches „s“.[21] (Eine weitere Stadt in Florida, City of Naples, hatte im vergangenen August bei einem ähnlichen BEC-Angriff 700.000 US-Dollar verloren.)

Vertreter von Ocala meldeten den Fall an ihre Versicherung, um einen Teil des Geldes zurückzuerhalten. Derzeit laufen strafrechtliche Ermittlungen.[22]

[18] Carlos E. Medina (Ocala StarBanner): „Ocala police: Scammers swiped nearly $750,000 from city“ (Polizei von Ocala: Betrüger erbeuten fast 750.000 USD von der Stadt), Oktober 2019.

[19] ebd.

[20] ebd.

[21] S. Rowe (Ocala Police Department): „Case Narrative, Incident: 201900183389“ (Bericht zum Fall 201900183389). Oktober 2019.

[22] WESH 2 News: „Police: Scammers swindled nearly $750,000 from city of Ocala“ (Polizei: Betrüger erbeuten fast 750.000 USD von Ocala), Oktober 2019.

10. Rijksmuseum Twenthe

Wenn Cyberkriminelle Banken, Unternehmen, Behörden und andere Ziele mit BEC- und EAC-Methoden betrügen, haben sie große Beute im Sinn. Daher überrascht es kaum, wenn sie Kunsthändler und Museen ins Visier nehmen, die mit wertvollen Meisterwerken zu tun haben.

Das Rijksmuseum Twenthe, ein Nationalmuseum im niederländischen Enschede, verlor 3,1 Millionen US-Dollar Euro an einen EAC-Betrüger, der als renommierter Londoner Kunsthändler auftrat. Das Museum verhandelte monatelang per E-Mail mit dem Händler, um das Gemälde „A View of Hampstead Heath: Child's Hill, Harrow in the Distance" des englischen Landschaftsmalers John Constable aus dem Jahre 1824 zu kaufen.[23]

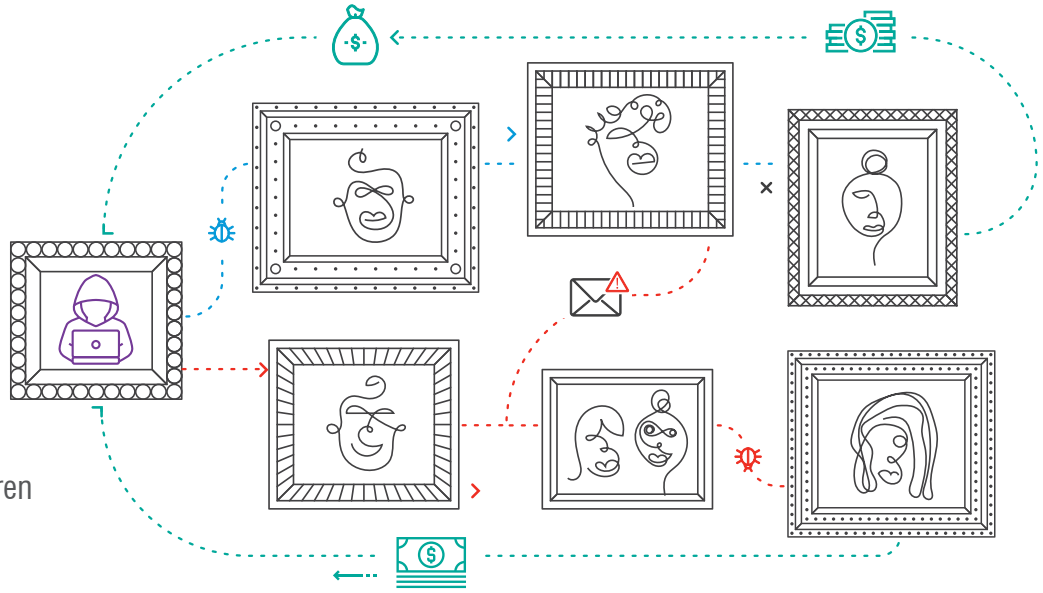
Irgendwann konnte ein Betrüger entweder das E-Mail-Konto des Kunsthändlers kapern oder eine überzeugende Doppelgänger-Adresse erstellen – diese Details sind Bestandteil des laufenden Gerichtsverfahrens – und wartete darauf, dass die Verhandlungen sich dem Abschluss näherten. Der Händler verschickte das Bild, doch die Überweisung ging an ein Konto in Hongkong und nicht an das des Verkäufers. Der Betrüger hatte in einer früheren E-Mail die Zahlungsdetails „aktualisiert".

Das Museum hat den Kunsthändler verklagt und behauptet, dieser hätte fahrlässig gehandelt oder nicht eingegriffen, als der Betrüger sein Konto kompromittiert hatte. Der Händler klagt im Gegenzug gegen das Museum und ist der Meinung, dass dort die Bankdaten vor der Überweisung hätten genauer überprüft werden sollen.

Aktuell bleibt das Gemälde im Bestand des Museums, während das Verfahren läuft.

3,1 Mio. US-Dollar

an einen falschen Kunsthändler verloren



[23] Ellen Milligan (Bloomberg): „Fraudsters Posing as Art Dealer Got Gallery to Pay Millions" (Falsche Kunsthändler lassen Museum einen Millionenbetrag zahlen), Januar 2020.

SCHLUSSFOLGERUNG UND EMPFEHLUNGEN

Wie diese Fälle zeigen, sind BEC- und EAC-Betrüger in der Wahl ihrer Ziele nicht wählerisch. Sie greifen Organisationen jeder Größe sowie Menschen auf jeder Stufe der Karriereleiter an.

BEC- und EAC-Angriffe lassen sich insbesondere mit veralteten Tools, nur punktuell ansetzenden Lösungen und den in Cloud-Plattformen integrierten Schutzmaßnahmen nur schwer erkennen und verhindern. BEC-E-Mails enthalten weder Malware noch schädliche URLs, die mit standardmäßiger Cyberabwehr analysiert werden könnten.

Zum Glück ist es nie zu spät – oder zu früh – für den Aufbau einer starken Abwehrstrategie gegen BEC/EAC. Da sich diese Angriffe gegen menschliche Schwächen und nicht gegen technische Schwachstellen richten, sind personenorientierte Sicherheitsmaßnahmen erforderlich, die ein großes Spektrum an BEC- und EAC-Techniken verhindern, erkennen und abwehren können.

Weitere Informationen zu BEC/EAC-Angriffen und ihrer Abwehr erhalten Sie unter **proofpoint.com/us/solutions/bec-and-eac-protection.**

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenorientierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0503-001-01-01 04/20