COMMERZBANK
Die Bank an Ihrer Seite

Fokusbericht

Cybersecurity

Kurzversion

Datenstand: 22.7.2019

Inhalt

Die grau markierten Kapitel sind in der Langversion des Berichtes enthalten.
Um die Langversion des Berichtes zu erhalten, nutzen Sie unseren Branchenservice oder sprechen Sie gerne Ihren Firmenkundenbetreuer an.

Hier geht es zum Branchenservice

Executive Summary

Absolute Sicherheit vor Angriffen aus dem Netz gibt es nicht. Cybersecurity kann jedoch die Risiken eines Angriffs und dessen negative Folgen minimieren. Ziel der Sicherheitsmaßnamen ist es daher, die Resilienz beziehungsweise Widerstandsfähigkeit des Unternehmens vor Cyberangriffen zu erhöhen. Dabei zeigt sich, dass der Schutz vor Cyberangriffen immer mit einer Abwägung von unterschiedlichen Unternehmenszielen verbunden ist.

Der Schutz gegen Cyberkriminalität beginnt mit dem Verständnis für die Gefahren beziehungsweise Risiken, denn es zeigt sich, dass die Schadprogramme und Methoden immer variantenreicher werden – was wiederum eine steigende Komplexität mit sich bringt.

Technische Maßnahmen wie ein Basisschutz – Passwortsicherung, Firewalls, Virenscanner, Updates und Back-ups – sind nahezu in allen Unternehmen vorhanden. Dieser Mindeststandard erweist sich aber angesichts der ständigen Weiterentwicklung auf der Seite der Angreifer als nicht ausreichend. Die IT-Technologie und -Infrastruktur sowie die Software-Anwendungen müssen daher permanent kontrolliert beziehungsweise aktualisiert werden. In regelmäßigen Abständen sollten Unternehmen darüber hinaus prüfen – auch durch bestellte Hackerangriffe – ob das Cybersecurity-Niveau noch ausreichend ist.

Hinsichtlich der organisatorischen Maßnahmen sollten bei der Cybersecurity klare personelle Verantwortlichkeiten festgelegt werden. Bei größeren Unternehmen ist die Einrichtung eines Chief Information Security Officers sinnvoll. Ebenso wichtig wie die Sensibilität der Führungskräfte für das Thema Cybersecurity ist die Aufmerksamkeit der Mitarbeiter. Es sollte ihnen vermittelt werden, dass sie durch ihr Handeln einen wichtigen Beitrag zum Schutz des Unternehmens liefern.

Für den Fall eines Angriffs sollte ein Notfallplan zur Verfügung stehen, um kritische Funktionen aufrechtzuerhalten und nach einem Angriff wieder schnell zur Normalität zurückzukehren. Der Plan sollte in analoger Form vorliegen. Für die Zeit danach gilt: Sobald ein finanzieller Schaden durch Erpressung oder Betrug entsteht, ist zur Schadensbegrenzung die Bank als erster Ansprechpartner zu nennen. Bei jedem Vorfall muss nach vorheriger interner Abstimmung die Polizei eingeschaltet werden. Schließlich gilt es, durch eine transparente interne und externe Kommunikation die beschädigte Reputation wiederherzustellen.

1. Es sollte ein normaler Tag sein

Es ist ein Montag. Herr Dr. Bottlich ist spät dran und eilt von der Tiefgarage seines Arbeitgebers hoch in sein Büro. Er ist kaufmännischer Leiter eines mittelständischen Unternehmens und steckt mit seiner Abteilung mitten im Jahresabschluss, sodass er einen anstrengenden Tag erwartet. Außerdem ist heute der Geburtstag seiner Frau. Der Tisch in ihrem Lieblingsrestaurant ist für abends schon reserviert. Daher möchte er das Büro heute nicht allzu spät verlassen.

Doch während er aus dem Aufzug in den Flur tritt, ist irgendetwas anders. Es ist ungewohnt still auf dem Gang. Wo sind seine Mitarbeiter? Die Sekretärin begrüßt ihn ganz aufgeregt und eilt ihm erklärend entgegen. „Die meisten haben wir in die Cafeteria geschickt. Ich bin ja so froh, dass Sie da sind, Herr Dr. Bottlich. Nichts geht mehr: Kein Telefon, kein Computer und die Webseite ist nicht erreichbar. Die IT ist schon informiert. In 10 Minuten soll es ein Krisenmeeting beim Chef geben.“ Die Menge an Informationen überrollt Herrn Dr. Bottlich, und er versteht die Lage sowie ihre Tragweite noch nicht. „Heißt das, die Produktion steht auch?“ – „Ja, alles – es heißt, dass wir wohl Opfer eines Verschlüsselungstrojaners wurden. Wir haben keinen Zugang mehr zu irgendwelchen Systemen oder Daten.“

Herr Dr. Bottlich legt Mantel und Tasche ab, eilt in die Etage der Geschäftsleitung. Dort ist der Ernst der Lage in den Gesichtern ablesbar; der Chef erklärt die Situation: „Fast alles ist verschlüsselt. Irgendwie haben Hacker eine Schadsoftware ins Unternehmen geschleust. Wie genau, dass steht noch nicht fest. Nur so viel ist bis jetzt klar: Der oder die Täter verlangen von uns 2 Millionen Euro, die wir in Bitcoins zahlen sollen. Erst nach dieser Zahlung bekommen wir einen Code zugeschickt, mit dem wir angeblich wieder alles entschlüsseln können.“ Es herrscht vollkommene Ratlosigkeit.

Fragen und Antworten eilen durch den Raum:
„Was ist mit den Backups?“ – „Auch verschlüsselt, das Meiste jedenfalls.“ – „Ist noch irgendetwas zur retten?“ – „Das wissen wir nicht genau. Es waren zwei verschiedene Server offline – aus Wartungsgründen. Wir überprüfen gerade, was dort gespeichert ist.“ – „Können wir die produzierten Maschinen der letzten Woche ausliefern?“ – „Nein. Wir haben keinen Zugriff auf die Verträge, Adressen und Frachtpapiere.“ – „Was machen wir mit den Logistikunternehmen, die auf dem Hof stehen?“ – Schulterzucken.

Nun denkt Herr Dr. Bottlich an seinen Jahresabschluss, der schon zu 75 Prozent fertig war. Er fragt den IT-Chef, was der jüngste Stand ist, der noch gesichert ist. Dieser schaut ihn aber nur an, als wäre er unwillig zu wiederholen, was er gerade zum Thema Back-ups gesagt hat.

Die Runde berät die nächsten Schritte: Wie informieren wir die Mitarbeiter? E-Mails und Intranet sind ja offline. Damit besteht auch kein Zugriff auf Organigramme und Telefonlisten. Ist der Angreifer noch im System? Was sagen wir Kunden und Lieferanten? Außerdem einigt man sich nach längerer Diskussion darauf, die Polizei zu informieren.

Für 12 Uhr wird das nächste Meeting ins Auge gefasst, bei dem man weiter beraten will, wie es weitergehen soll. Dann muss auch entschieden werden, ob man die Mitarbeiter für heute nach Hause schickt.

Jeder bekommt zum Schluss noch den Auftrag, bis dahin eine Liste mit allen Mitarbeitern seiner Abteilung und deren Erreichbarkeit anzufertigen. „Für die IT übernimmst Du das bitte, Jürgen. Die haben jetzt anderes zu tun. Wir brauchen Namen, Abteilung, Handynummern und private E-Mail-Adressen.“ Herr Dr. Bottlich fragt noch, ob die Bank informiert werden soll. „Nur das nichts passiert.“ – „Gute Idee. Aber bitte noch kein Wort über die Details.“

Herr Dr. Bottlich geht in sein Büro. Als Erstes sucht er die Visitenkarte seines Bankers, findet sie aber nicht. Deshalb sucht er über den Browser seines Smartphones die allgemeine Hotline der Bank. Über diese landet er im zentralen Callcenter der Bank – irgendwo in Deutschland. Er versucht sich zu seinem Berater durchstellen zu lassen, was nach mehreren Anläufen auch gelingt. Der Bankangestellte ist allerdings verwundert. „Sind Sie es wirklich, Herr Dr. Bottlich? Die Nummer, von der aus Sie anrufen, kenne ich nicht. Und wieso kommen Sie überhaupt über die Hotline rein und haben nicht direkt angerufen? Ich bin etwas verunsichert. Darf ich Sie gleich zurückrufen? Ich schaue gerade in unserem System nach Ihren Kontaktdaten.“

Es vergeht etwas Zeit und sein Berater meldet sich wieder – auf dem Handy. Denn auf dem Festnetz ist trotz Freizeichen keiner ans Telefon gegangen.

Dies ist zwar eine fiktive Geschichte, die sich aber in ähnlicher Form in der Realität in mehreren Firmen 2018 und 2019 so abgespielt hat. Ohne funktionierende Back-ups brauchen betroffene Unternehmen Wochen, ja Monate, um einen vollständigen Normalbetrieb wiederherzustellen. Und selbst dann sind Daten dabei meist für immer verloren.

Nach mehreren Tagen ohne Aussicht auf Erfolg ist in fast allen betroffenen Unternehmen der Tiefpunkt erreicht und die Aussichtslosigkeit so groß, dass sich einige der Firmen auch mit dem Gedanken abfinden, der Erpressung nachzugeben. Sie hoffen auf den „Schlüssel", der alles wieder rückgängig macht. Für einige Firmen beginnt mit solch einem Tag der Weg in die Krise und letztlich in die Insolvenz.

Grundsätzlich ist die Wahrscheinlichkeit, unabhängig von Branche und Größe des Unternehmens Ziel eines Cyberangriffs zu werden, extrem hoch. Cybersecurity ist daher ein Thema, mit dem sich jedes Unternehmen zwingend auseinandersetzen muss. Denn es betrifft keinesfalls nur große Konzerne oder Internetfirmen.

Erst mit Cybersecurity können Unternehmen das gesamte Potenzial der Digitalisierung realisieren.

Dieser Fokusbericht widmet sich der Sicherheit Ihres Unternehmens und zeigt Ihnen eine Vielzahl an Möglichkeiten, wie Sie sich und Ihre Firma in unternehmerischer Verantwortung vor solch einem Szenario schützen können.

Der Schutz gegen Cyberkriminalität beginnt dabei mit dem Verständnis für die Gefahren beziehungsweise Risiken. Dies sind neue Gefahren, auf die sich die Unternehmen im Zuge der Digitalisierung einstellen müssen. Die Vielzahl an vernetzten Geräten und digitalen Kanälen führt dazu, dass nahezu alles ein potenzielles Ziel ist und eröffnet den (Cyber-)Kriminellen nie dagewesene Einfallstore.

Commerzbank Research Für die Erstellung dieser Ausarbeitung ist das Segment Firmenkunden der Commerzbank AG, Frankfurt am Main, verantwortlich.

Die Verfasser bestätigen, dass die in diesem Dokument geäußerten Einschätzungen ihre eigenen Einschätzungen genau wiedergeben und kein Zusammenhang zwischen ihrer Dotierung – weder direkt noch indirekt noch teilweise – und den jeweiligen, in diesem Dokument enthaltenen Empfehlungen oder Einschätzungen bestand, besteht oder bestehen wird. Der (bzw. die) in dieser Ausarbeitung genannte(n) Analyst(en) ist (sind) nicht bei der FINRA als Research-Analysten registriert/qualifiziert. Solche Research-Analysten sind möglicherweise keine assoziierten Personen der Commerz Markets LLC und unterliegen daher möglicherweise nicht den Einschränkungen der FINRA Rule 2241 in Bezug auf die Kommunikation mit einem betroffenen Unternehmen, öffentliche Auftritte und den Handel mit Wertpapieren im Bestand eines Analysten.

Disclaimer Dieses Dokument dient ausschließlich zu Informationszwecken und berücksichtigt nicht die besonderen Umstände des Empfängers. Es stellt keine Anlageberatung dar. Die Inhalte dieses Dokuments sind nicht als Angebot oder Aufforderung zum Kauf oder Verkauf von Wertpapieren oder irgendeiner anderen Handlung beabsichtigt und dienen nicht als Grundlage oder Teil eines Vertrages. Anleger sollten sich unabhängig und professionell beraten lassen und ihre eigenen Schlüsse im Hinblick auf die Eignung der Transaktion einschließlich ihrer wirtschaftlichen Vorteilhaftigkeit und Risiken sowie ihrer Auswirkungen auf rechtliche und regulatorische Aspekte sowie Bonität, Rechnungslegung und steuerliche Aspekte ziehen.

Die in diesem Dokument enthaltenen Informationen sind öffentliche Daten und stammen aus Quellen, die von der Commerzbank als zuverlässig und korrekt erachtet werden. Die Commerzbank übernimmt keine Garantie oder Gewährleistung im Hinblick auf Richtigkeit, Genauigkeit, Vollständigkeit oder Eignung für einen bestimmten Zweck. Die Commerzbank hat keine unabhängige Überprüfung oder Due Diligence öffentlich verfügbarer Informationen im Hinblick auf einen unverbundenen Referenzwert oder -index durchgeführt. Alle Meinungsaussagen oder Einschätzungen geben die aktuelle Einschätzung des Verfassers bzw. der Verfasser zum Zeitpunkt der Veröffentlichung wieder und können sich ohne vorherige Ankündigung ändern. Die hierin zum Ausdruck gebrachten Meinungen spiegeln nicht zwangsläufig die Meinungen der Commerzbank wider. Die Commerzbank ist nicht dazu verpflichtet, dieses Dokument zu aktualisieren, abzuändern oder zu ergänzen oder deren Empfänger auf andere Weise zu informieren, wenn sich ein in diesem Dokument genannter Umstand oder eine darin enthaltene Stellungnahme, Schätzung oder Prognose ändert oder unzutreffend wird.

Diese Ausarbeitung kann Handelsideen enthalten, im Rahmen derer die Commerzbank mit Kunden oder anderen Geschäftspartnern in solchen Finanzinstrumenten handeln darf. Die hier genannten Kurse (mit Ausnahme der als historisch gekennzeichneten) sind nur Indikationen und stellen keine festen Notierungen in Bezug auf Volumen oder Kurs dar. Die in der Vergangenheit gezeigte Kursentwicklung von Finanzinstrumenten erlaubt keine verlässliche Aussage über deren zukünftigen Verlauf. Eine Gewähr für den zukünftigen Kurs, Wert oder Ertrag eines in diesem Dokument genannten Finanzinstruments oder dessen Emittenten kann daher nicht übernommen werden. Es besteht die Möglichkeit, dass Prognosen oder Kursziele für die in diesem Dokument genannten Unternehmen bzw. Wertpapiere aufgrund verschiedener Risikofaktoren nicht erreicht werden. Hierzu zählen in unbegrenztem Maße Marktvolatilität, Branchenvolatilität, Unternehmensentscheidungen, Nichtverfügbarkeit vollständiger und akkurater Informationen und/oder die Tatsache, dass sich die von der Commerzbank oder anderen Quellen getroffenen und diesem Dokument zugrunde liegenden Annahmen als nicht zutreffend erweisen.

Die Commerzbank und/oder ihre verbundenen Unternehmen dürfen als Market Maker in den(m) Instrument(en) oder den entsprechenden Derivaten handeln, die in unseren Research-Studien genannt sind. Mitarbeiter der Commerzbank oder ihrer verbundenen Unternehmen dürfen unseren Kunden und Geschäftseinheiten gegenüber mündlich oder schriftlich Kommentare abgeben, die von den in dieser Studie geäußerten Meinungen abweichen. Die Commerzbank darf Investmentbanking-Dienstleistungen für in dieser Studie genannte Emittenten ausführen oder anbieten.

Weder die Commerzbank noch ihre Geschäftsleitungsorgane, leitenden Angestellten oder Mitarbeiter übernehmen die Haftung für Schäden, die ggf. aus der Verwendung dieses Dokuments, seines Inhalts oder in sonstiger Weise entstehen.

Die Aufnahme von Hyperlinks zu den Websites von Organisationen, die in diesem Dokument erwähnt werden, impliziert keineswegs eine Zustimmung, Empfehlung oder Billigung der Informationen der Websites bzw. der von dort aus zugänglichen Informationen durch die Commerzbank. Die Commerzbank übernimmt keine Verantwortung für den Inhalt dieser Websites oder von dort aus zugänglichen Informationen oder für eventuelle Folgen aus der Verwendung dieser Inhalte oder Informationen.

Dieses Dokument ist nur zur Verwendung durch den Empfänger bestimmt. Es darf weder in Auszügen noch als Ganzes ohne vorherige schriftliche Genehmigung der Commerzbank auf irgendeine Weise verändert, vervielfältigt, verbreitet, veröffentlicht oder an andere Personen weitergegeben werden. Die Art und Weise, wie dieses Produkt vertrieben wird, kann in bestimmten Ländern, einschließlich der USA, weiteren gesetzlichen Beschränkungen unterliegen. Personen, in deren Besitz dieses Dokument gelangt, sind verpflichtet, sich diesbezüglich zu informieren und solche Einschränkungen zu beachten. Mit Annahme dieses Dokuments stimmt der Empfänger der Verbindlichkeit der vorstehenden Bestimmungen zu.

Zusätzliche Informationen für Kunden in folgenden Ländern:
Deutschland: Die Commerzbank AG ist im Handelsregister beim Amtsgericht Frankfurt unter der Nummer HRB 32000 eingetragen. Die Commerzbank AG unterliegt der Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Graurheindorfer Straße 108, 53117 Bonn, Marie-Curie-Straße 24-28, 60439 Frankfurt am Main und der Europäischen Zentralbank, Sonnemannstraße 20, 60314 Frankfurt am Main, Deutschland.

Großbritannien: Dieses Dokument wurde von der Commerzbank AG, Filiale London, herausgegeben oder für eine Herausgabe in Großbritannien genehmigt. Die Commerzbank AG, Filiale London, ist von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) und von der Europäischen Zentralbank amtlich zugelassen und unterliegt nur in beschränktem Umfang der Regulierung durch die Financial Conduct Authority und Prudential Regulation Authority. Einzelheiten über den Umfang der Genehmigung und der Regulierung durch die Financial Conduct Authority und Prudential Regulation Authority erhalten Sie auf Anfrage. Diese Ausarbeitung richtet sich ausschließlich an „Eligible Counterparties" und „Professional Clients". Sie richtet sich nicht an „Retail Clients". Ausschließlich „Eligible Counterparties" und „Professional Clients" ist es gestattet, die Informationen in dieser Ausarbeitung zu lesen oder sich auf diese zu beziehen. Commerzbank AG, Filiale London bietet nicht Handel, Beratung oder andere Anlagedienstleistungen für „Retail Clients" an.

USA: Die Commerz Markets LLC („Commerz Markets") hat die Verantwortung für die Verteilung dieses Dokuments in den USA unter Einhaltung der gültigen Bestimmungen übernommen. Wertpapiertransaktionen durch US-Bürger müssen über die Commerz Markets, Swaptransaktionen über die Commerzbank AG abgewickelt werden. Nach geltendem US-amerikanischen Recht können Informationen, die Commerz Markets-Kunden betreffen, an andere Unternehmen innerhalb des Commerzbank-Konzerns weitergegeben werden. Sofern dieses Dokument zur Verteilung in den USA freigegeben wurde, ist es ausschließlich nur an „US Institutional Investors" und „Major Institutional Investors" gerichtet, wie in Rule 15a-6 unter dem Securities Exchange Act von 1934 beschrieben. Commerz Markets ist Mitglied der FINRA und SIPC. Die Commerzbank AG ist bei der CFTC vorläufig als Swaphändler registriert.

Kanada: Die Inhalte dieses Dokuments sind nicht als Prospekt, Anzeige, öffentliche Emission oder Angebot bzw. Aufforderung zum Kauf oder Verkauf der beschriebenen Wertpapiere in Kanada oder einer kanadischen Provinz bzw. einem kanadischen Territorium beabsichtigt. Angebote oder Verkäufe der beschriebenen Wertpapiere erfolgen in Kanada ausschließlich im Rahmen einer Ausnahme von der Prospektpflicht und nur über einen nach den geltenden Wertpapiergesetzen ordnungsgemäß registrierten Händler oder alternativ im Rahmen einer Ausnahme von der Registrierungspflicht für Händler in der kanadischen Provinz bzw. dem kanadischen Territorium, in dem das Angebot abgegeben bzw. der Verkauf durchgeführt wird. Die Inhalte dieses Dokuments sind keinesfalls als Anlageberatung in einer kanadischen Provinz bzw. einem kanadischen Territorium zu betrachten und nicht auf die Bedürfnisse des Empfängers zugeschnitten. In Kanada sind die Inhalte dieses Dokuments ausschließlich für Permitted Clients (gemäß National Instrument 31-103) bestimmt, mit denen Commerz Markets LLC im Rahmen der Ausnahmen für internationale Händler Geschäfte treibt. Soweit die Inhalte dieses Dokuments sich auf Wertpapiere eines Emittenten beziehen, der nach den Gesetzen Kanadas oder einer kanadischen Provinz bzw. eines kanadischen Territoriums gegründet wurde, dürfen Geschäfte in solchen Wertpapieren nicht durch Commerz Markets LLC getätigt werden. Keine Wertpapieraufsicht oder ähnliche Aufsichtsbehörde in Kanada hat dieses Material, die Inhalte dieses Dokuments oder die beschriebenen Wertpapiere geprüft oder genehmigt; gegenteilige Behauptungen zu erheben, ist strafbar.

Europäischer Wirtschaftsraum: Soweit das vorliegende Dokument durch eine außerhalb des Europäischen Wirtschaftsraumes ansässige Rechtsperson erstellt wurde, erfolgte eine Neuausgabe für die Verbreitung im Europäischen Wirtschaftsraum durch die Commerzbank AG, Filiale London.

Singapur: Dieses Dokument wird in Singapur von der Commerzbank AG, Filiale Singapur, zur Verfügung gestellt. Es darf dort nur von institutionellen Investoren laut Definition in Section 4A des Securities and Futures Act, Chapter 289, von Singapur („SFA") gemäß Section 274 des SFA entgegengenommen werden.

Hongkong: Dieses Dokument wird in Hongkong von der Commerzbank AG, Filiale Hongkong, zur Verfügung gestellt und darf dort nur von „professionellen Anlegern" im Sinne von Schedule 1 der Securities and Futures Ordinance (Cap. 571) von Hongkong und etwaigen hierin getroffenen Regelungen entgegengenommen werden.

Japan: Dieses Dokument und seine Verteilung stellen keine „Aufforderung" gemäß dem Financial Instrument Exchange Act (FIEA) dar und sind nicht als solche auszulegen. Dieses Dokument darf in Japan ausschließlich an „professionelle Anleger" gemäß Section 2(31) des FIEA und Section 23 der Cabinet Ordinance Regarding Definition of Section 2 of the FIEA durch die Commerzbank AG, Tokyo Branch, verteilt werden. Die Commerzbank AG, Tokyo Branch, war jedoch nicht an der Erstellung dieses Dokuments beteiligt. Nicht alle Finanz- oder anderen Instrumente, auf die in diesem Dokument Bezug genommen wird, sind in Japan verfügbar. Anfragen bezüglich der Verfügbarkeit dieser Instrumente richten Sie bitte an die Abteilung Corporates & Markets der Commerzbank AG oder an die Commerzbank AG, Tokyo Branch. [Commerzbank AG, Tokyo Branch] Eingetragenes Finanzinstitut: Director of Kanto Local Finance Bureau (Tokin) Nr. 641 / Mitgliedsverband: Japanese Bankers Association.

Australien: Die Commerzbank AG hat keine australische Lizenz für Finanzdienstleistungen. Dieses Dokument wird in Australien an Großkunden unter einer Ausnahmeregelung zur australischen Finanzdienstleistungslizenz von der Commerzbank gemäß Class Order 04/1313 verteilt. Die Commerzbank AG wird durch die BaFin nach deutschem Recht geregelt, das vom australischen Recht abweicht.

Beratung
und Terminvereinbarung für Firmenkunden

Filialen

Die Commerzbank ist an mehr als 100 Standorten für Firmenkunden in Deutschland und weltweit in knapp 50 Ländern vor Ort vertreten.

Online

www.commerzbank.de/firmenkunden

Commerzbank AG
Zentrale
Kaiserplatz
Frankfurt am Main

Postanschrift
60261 Frankfurt am Main
SectorDesk@commerzbank.com

Der Bericht beruht auf Analysen und Einschätzungen durch die Commerzbank AG.

Die redaktionelle und grafische Aufbereitung des Berichts erfolgt in Kooperation mit dem Handelsblatt Research Institute.

Dieser Bericht wurde im Juli 2019 erstellt.