https://blz.li/398v

Leine Blitz
blitzschnell informiert

WAS HABEN CORONA UND RANSOMWARE IN DER WEIHNACHTSZEIT GEMEINSAM?

Veröffentlicht am 20.12.2021 um 08:31 von Reinhard Kroll

Weihnachten 2021 und das Coronavirus hat die Welt weiterhin im Griff. Das Virus mutiert, passt sich an veränderte Bedingungen an und wird resistenter. Zahlreiche Lieferketten sind bereits unter den ersten Corona-Wellen zusammengebrochen, andere drohen zusammen zu brechen. Alle Branchen sind vom Virus betroffen, einige, wie die Logistikbranche, besonders schwer. Die Unternehmen und ihre Angestellten operieren länderübergreifend und müssen unterschiedliche Auflagen von unterschiedlichen Regierungen beachten. Die zahlreichen Lockdowns, die regionalen Unterschiede bei der Akzeptanz von Impfstoffen, die Schließung von Grenzübergängen oder die Wiedereinführung von Grenzkontrollen führen zu Verzögerungen beim Warentransport. Branchen, die abhängig von funktionierenden Lieferketten sind, wie die Automobilindustrie, fehlen Bauteile, insbesondere Halbleiter und andere Chips. Das Unternehmen Tesla hat deshalb zahlreiche Autos ohne USB-Anschlüsse ausgeliefert.Während die Weltwirtschaft versucht, sich unter den erschwerten Bedingungen neu aufzustellen und das Arbeiten aus dem Homeoffice für viele Beschäftigte zum gegenwärtigen Standard wurde, versuchen Kriminelle, die aktuelle Situation für sich zu nutzen. Während IT-Abteilungen ihre Ressourcen dafür nutzen, die IT an die veränderte Situation anzupassen und allen Mitarbeitern das Arbeiten von zu Hause aus zu ermöglichen, sind ihre Ressourcen gebunden und auf Angriffe kann kaum reagiert werden.In den vergangenen Jahren ist die Anzahl der gemeldeten Angriffe stetig gestiegen. Insgesamt belief sich der geschätzte Schaden in den Jahren 2018 und 2019 auf jeweils 103 Milliarden Euro. Seit der Corona Pandemie hat sich die Schadenssumme mehr als verdoppelt auf geschätzt 220 Milliarden Euro. Die Mehrheit der Angriffe erfolgte durch Ransomware Angriffe (31 Prozent) und DDoS Angriffe (27 Prozent). In diesem Jahr ist die Anzahl der Ransomware Angriffe im Vergleich zum Vorjahr um 25 Prozent angestiegen. (Siehe Infografik) Auch wenn im dritten Quartal erstmals die Anzahl der gemeldeten Ransomware Angriffe gesunken ist, sehen unabhängige Stellen keine Entlastung. Der TÜV SÜD hat kürzlich seine Trends im Bereich Cybersecurity für 2022 veröffentlicht und prognostiziert weitere Ransomware Angriffe. Er begründet dies mit der Professionalisierung der Angreifer, welche ihre Dienste als Cybercrime-as-a-Service für jedermann bereitstellen. Zahlreiche Angriffe in den vergangenen Wochen, unter anderem auf Media Markt und Saturn, wodurch die Kassensysteme nicht mehr funktionierten, sowie auf den Maschinenbauer Bucher und den Krypto Broker Robinhood scheinen diese Einschätzung zu bestätigen.Zusätzlich ist Emotet, die bekannteste Ransomware des Planeten, zurück gekehrt, welche allein in Deutschland im Jahr 2020 einen Schaden in Höhe von 14,5 Millionen Euro verursacht hat. Für die Weihnachtszeit erwarten deshalb das BSI und BKA in Hinblick auf das erneute Auftauchen von Emotet weitere Cyberattacken. "Insbesondere Feiertage, Urlaubszeiten und auch Wochenenden wurden in der Vergangenheit wiederholt für solche Angriffe genutzt, da viele Unternehmen und Organisationen dann weniger reaktionsfähig sind", wird Arne Schönbohm, BSI-Präsident, in einer aktuellen Warnung des BSI, vom 2. Dezember, zitiert. Ähnlich wie die neuen Mutationen des Corona Virus hat Emotet sich ebenfalls weiterentwickelt und ist jetzt resistenter. Die Schadsoftware verschlüsselt die Kommunikation mit selbsterstellten Zertifikaten und ist auf infizierten Systemen schwerer zu entdecken.Das BSI und BKA empfehlen Unternehmen und Organisationen daher, ihre Alarmierungsprozesse und Notfallkonzepte zu üben und funktionsfähige Backups

bereitzuhalten.Damit Unternehmen im Ernstfall handlungsfähig sind, ist es wichtig, Abläufe zu besprechen, zu üben und zu dokumentieren. Unternehmen können sich idealerweise in Nicht-Krisenzeiten auf außergewöhnliche Situationen vorbereiten, wenn Beteiligte sich in keiner Stress- oder Drucksituation befinden. Denn während eines Notfalls oder einer Krise haben alle (relevanten) Beteiligten keine Zeit für eine sorgfältige und umfassende Planung von Entscheidungen und profitieren erheblich von erstellten und vorbereiteten Unterlagen und geübten Abläufen. Denn akute Vorfälle müssen aktiv behandelt werden und erlauben keinen zeitlichen Aufschub.Zusätzlich wollen relevante Stakeholder wie Kunden, Partner(-unternehmen) und Presse informiert sein und haben eine hohe Erwartungshaltung an die Krisenkommunikation.Um auf einen Vorfall also tatsächlich gut vorbereitet zu sein, dürfen Unternehmen keine Zeit mit Routineaufgaben verlieren. Um aktiv handlungsfähig zu sein, ist es von größter Wichtigkeit, eine aktuelle Dokumentation und erprobte Abläufe zu haben. Unternehmen können sich Alarmierungsketten und Kriterien, wann diese anzuwenden sind, mithilfe von Fragen erarbeiten. Was ist für unser Unternehmen ein meldepflichtiger Vorfall? Wer ist für den aktuellen Vorfall zu alarmieren? In welchen Räumlichkeiten wird die Lage beurteilt? Welche Sofortmaßnahmen können ergriffen werden? Wer informiert relevante Stakeholder über den Vorfall und welche Informationen werden mitgeteilt?Darüber hinaus können Unternehmen noch weitere technische Unterlagen erstellen. Hierzu gehören Backup- und Wiederanlaufpläne für Systeme, um diese komplett neu aufsetzen oder aus einem Backup wiederherstellen zu können, sowie eine Reihenfolge, in welcher ausgefallene Systeme wieder starten können. Bei allen aufgezeigten Fragen hilft idealerweise Software, wie zum Beispiel INDART® Professional, bei der Erfassung von kritischen Systemen für Kernprozesse eines Unternehmens und bei der Dokumentation von Alarmierungsketten und Wiederanlaufplänen, so dass alle Daten im Krisenfall auch zur Verfügung stehen.