Deaktivierte Firewall infolge der Kündigung des IT-Leiters?

Mechanische Sicherungsmaßnahmen sind wie die Schließanlage der Geschäftsräume zur Einbruchvorsorge elementare Bestandteile der IT-Sicherheit in Unternehmen. Auch diese können natürlich nur unter der Voraussetzung einer kontinuierliche Anwendung und Pflege, beispielsweise durch Updates der Firewall mit Echtzeit-Daten zu aktuellen Bedrohungen und Angriffen, einen verlässlichen Beitrag zur Netzwerksicherheit leisten. Das Potential für menschliches Versagen oder sogar vorsätzliches Verschulden ist dabei zu berücksichtigen.

Der konkrete Fall aus 2020

Unser Kunde, ein inhabergeführter Logistikdienstleister mit mehreren Standorten in Europa, stellte fest, dass über mehrere Tage hinweg die Arbeitsgeschwindigkeit aller PCs und des Server immer langsamer wurden, bis man eines Tages gar nicht mehr arbeiten konnte. Der IT-affine Geschäftsführer mit Programmierfähigkeiten startete in der eigenen Haustechnik der EDV zu recherchieren und befürchtete anfangs, dass der von ihm gekündigte IT-Abteilungsleiter kurz vor seinem Ausscheiden das Unternehmen in irgendeiner Form durch einen vorsätzlichen internen Hackerangriff noch schädigen wollte. Später stellte sich heraus, dass dem glücklicherweise nicht so war.

Dem Kunden drohten somit eine Betriebsunterbrechung und Haftungsansprüche, welche einen erheblichen finanziellen Schaden bewirken können. Zu den drohenden monetären Schäden kommen natürlich noch die internen Aufwände wie Erkennung, Aufklärung und Lösung.

Das Unternehmen verfügt nach vollständiger Realisierung eines afm Risikoplans über eine spezielle Cyberversicherung, die auch forensische Dienstleistung mit einschließt. Somit konnten wir in dem vorliegenden Fall kurzfristig Kontakt zu einem der führenden Beratungshäuser für Security und IT-Management (Partner der Cyberversicherung), hergestellt werden. Die Experten nahmen noch am gleichen Tage die forensische Recherche vor Ort auf und durchsuchten die EDV-Systeme nach Schadsoftware und potentiellen Sicherheitslücken. Parallel wurde durch unser Haus eine Schadensmeldung an den Risikoträger der Cyberversicherung gefasst, um sicherzustellen, dass die mit der Beauftragung des IT-Beratungshauses verursachten Kosten und Ausgaben im Sinne der Cyber-Versicherungsbedingungen für den Kunden übernommen werden.

Nach einigen Tagen der intensiven Recherche der Experten stellte sich heraus, dass die Firewall eines Routers manipuliert wurde. Wie und wodurch diese manipuliert wurde, konnte nicht eindeutig geklärt werden. Die Firewall war jedoch durch externen Zugriff deaktiviert worden. Die Sicherheitslücke konnte technisch geschlossen werden und das Unternehmen war wieder uneingeschränkt arbeitsfähig. Weitere potentielle Schäden und Beeinträchtigungen des Geschäftsergebnisses des Kunden konnten durch die schnelle und professionelle Herangehensweise vermieden werden.

Nach Prüfung des Vorganges und mit dem durch das IT-Beratungshaus erstellten technischen Abschlussberichtes wurde bestätigt, dass die entstandenen Kosten bedingungsgemäß versichert sind. Die von der Cyberversicherung übernommene Kostenrechnung der Experten betrug in diesem Fall ca. 8.000 Euro. Aber viel wichtiger: Ein potentiell wirtschaftlich schmerzhafter Schaden konnte für den Logistikdienstleister insgesamt vermieden werden – dank der von afm gebotenen Cyberversicherung, die ein hochprofessionelles Dienstleistungspaket einschließt. Der Geschäftsführer unseres Kunden drückte aufgrund des Erlebten seine besondere Dankbarkeit unter Anderem damit aus, dass er seine Emotionen wie folgt zum Ausdruck brachte:

„Das ist die erste Versicherung die wirklich bezahlt, wenn man sie dringend braucht“.