Erpressung bei einem Softwarehersteller für Handelsplattformen

Die Gefahr für Unternehmen durch Cyberkriminalität nimmt dramatisch zu. Cyberkriminelle nutzen vermehrt auch eine Taktik, um Unternehmen durch Datenverschlüsselung zu erpressen. Zahlen die Opfer nicht, landen die Informationen im Netz und führen zu hohen Haftungs- und Reputationsschäden. Häufig führen auch vertrieblich sinnvolle Angebote, beispielsweise Testbereichen auf Unternehmensseiten, zu potentiellen Gefahren, die Täter dazu veranlasst, an Unternehmen mit Forderungen heranzutreten.

Der konkrete Fall aus 2020

Unser Kunde ist ein Softwarehersteller, der hierbei auch Handelsplattformen entwickelt und potentiellen Interessenten die Testung der Funktionsweise der angebotenen Plattformen in der Umgebung der hauseigenen Homepage ermöglicht. Per E-Mail wendete sich der Erpresser an das Unternehmen, einige Sicherheitslücken entdeckt zu haben und drohte diese ins Internet zu stellen.

Für den Kunden bestand also eine äußerst unangenehme Situation mit der Bedrohung durch existenzgefährdender Kosten und Reputationsrisiken.

Das Unternehmen verfügt nach vollständiger Realisierung eines afm Risikoplans über eine spezielle Cyberversicherung, die auch forensische Dienstleistung mit einschließt. Im Zuge dessen konnten wir in kürzester Zeit Kontakt zwischen dem Softwarehersteller und den Experten einem der führenden Beratungshäuser für Security und IT-Management (Partner der Cyberversicherung) herstellen. Innerhalb weniger Tage analysierten die Experten den Quellcode des Softwareunternehmens und betreuten parallel im Hintergrund die rechtliche Beratung des Kunden zur Formulierung der Antworten auf die E-Mails des Erpressers. Darüber hinaus wurde versucht, die Sicherheitslücke zu finden, um weitere Erpressungen dieser Art und dergleichen Ursache auszuschließen. Es entwickelte sich ein digitaler Schriftverkehr zwischen dem Erpresser und dem Unternehmen. Parallel wurde durch unseren guten Kontakten im Hause der Cyberversicherung die Kostenübernahme für diese Erpressung geklärt.

Auf Anraten baute das Softwareunternehmen für den Erpresser eine neue Test-Umgebung, mit eigenem Rechenkern und verlangte auf dieser technischen Basis vom Erpresser den Nachweis anzutreten, die behaupteten Sicherheitslücken zu beweisen und bei erfolgreicher Beweisführung die von ihm verlangte Belohnung, das Lösegeld zu zahlen. Ziel dieser Aktion war es, dem Erpresser eine bedeutende Aufmerksamkeit zu schenken und Zeit zu gewinnen, um die vermeintliche Sicherheitslücke durch intensive Recherche der Software zu finden. Die von dem Erpresser behauptete Sicherheitslücke konnte nicht gefunden werden.

Nach einigen Wochen stellte sich heraus, dass der Erpresser hoch gepokert hatte, aber die behaupteten Sicherheitslücken dem Softwareunternehmen nicht beweisen konnte. Infolgedessen kam es nicht zur Bezahlung einer Belohnung oder von Erpressungsgeld. Der Kontakt zwischen dem Unternehmen und dem Erpresser riss ab.

Nicht unwesentlich war die Freude des Softwareunternehmens darüber, dass die Versicherung einige kleine Sicherheitslücken, andere als die vom Erpresser behaupteten, in dem Quellcode der Software mittels Programmierung beseitigen konnten.

Sämtliche entstandenen Kosten für eine vierwöchige praktische Schadenfallbegleitung und Abwicklung hat die Cyberversicherung gemäß den zugrundeliegenden Versicherungsbedingungen erstattet. Und noch wichtiger: Ein potentiell wirtschaftlich schmerzhafter Schaden konnte für den Softwarehersteller insgesamt vermieden werden – dank der von afm gebotenen Cyberversicherung, die ein hochprofessionelles Dienstleistungspaket einschließt.