KRZ.AKTUELL

SONDERAUSGABE November 2020

SÜDWESTDEUTSCHLAND

IT-Security im Wandel – vom Kostenfaktor zur (Über-)Lebensversicherung

Die fast täglichen Schlagzeilen über immer neue Ransomware*-Angriffe auf Großunternehmen, Krankenhäuser oder Universitäten sind deutliche Zeichen dafür, dass sich die Bedrohungslage in den letzten Jahren und Monaten geändert hat. Noch vor 3 - 4 Jahren zu Zeiten von „Locky“-Ransomware waren die Angriffe breit gestreut und durch Zahlung von relativ moderaten Lösegeldsummen von 300 - 500 Euro bekamen Opfer den Nachschlüssel, um wieder an die private Fotosammlung – aber auch an die Daten auf dem verschlüsselten Firmen-Dateiserver zu gelangen. Doch dann fingen die Cyberkriminellen vermehrt an, sich auf die wirklich lukrativen Ziele, auf Unternehmen und andere große Organisationen zu konzentrieren.

Eine von Sophos im Mai 2020 veröffentlichte Studie zum Thema Ransomware hat ergeben, dass über die Hälfte der in Deutschland befragten mittelständischen Unternehmen in den letzten 12 Monaten Opfer von Ransomware waren und bei diesen Unternehmen im Durchschnitt über 400.000 Euro Schaden durch den Ausfall oder die Einschränkung des Geschäftsbetriebs entstanden. Ein Cyberangriff ist also nicht mehr wie in vergangenen Jahrzehnten die Ausnahme – er ist heute die Regel und betrifft Organisationen aller Größen. Zudem haben die Cyberkriminellen die Taktik geändert. Nach einer erfolgreichen Infektion werden nicht gleich Daten mit einer Ransomware verschlüsselt. Stattdessen werden Unternehmensnetze erst langsam und vorsichtig ausgespäht, um Geschäftsgeheimnisse zu identifizieren, damit sich die Hacker im Netzwerk auf möglichst vielen Systemen einnisten können. Und bevor die Hacker dann mit einer Ransomware tatsächlich Backups löschen, Rechner verschlüsseln und das Unternehmen teilweise oder komplett lahmlegen, stehlen die Hacker zunächst Geschäftsgeheimnisse und personenbezogene Daten. Denn wenn die Hacker losschlagen und per Ransomware Rechner und Daten verschlüsseln, haben sie als weiteres Druckmittel die bereits gestohlenen Daten und drohen mit deren Veröffentlichung, falls das betroffene Unternehmen z. B. aufgrund eines guten Backup-Konzepts das Ransomware-Lösegeld nicht zahlen will. Denn mit der Veröffentlichung der gestohlenen Daten drohen dem Unternehmen Reputationsverlust, Schaden durch Preisgabe von Geschäftsgeheimnissen und nicht zuletzt Strafen im Rahmen der DSGVO, wenn personenbezogene Daten veröffentlicht wurden. Nicht umsonst nennt das Bundeskriminalamt in seinem im September 2020 erschienenen Cybercrime Bundeslagebild 2019 die Ransomware als „die primäre, existentielle Bedrohung für Unternehmen“.

Es stellt sich die Frage, was Organisationen tun können (und müssen), um nicht das nächste Opfer zu werden. Außer Frage steht, dass die traditionellen Schutzmaßnahmen wie Firewall und Anti-Virus heute keinen Schutz mehr gegen professionelle Angreifer bieten, die diese Hürden mit Leichtigkeit überwinden können. Der Bundesverband IT-Sicherheit e.V. (TeleTrusT), der u.a. maßgeblich auf die Einschätzungen der Cyberrisikoversicherungen einwirkt, definiert als „Stand der Technik“ im Jahr 2020 „Endpoint Detection & Response“ – abgekürzt EDR. EDR ist ein ganzheitlicher Ansatz am Endpoint und Server, der neben modernen Schutzmechanismen wie Exploit- und Ransomware-Schutz auch die unternehmensweite Erkennung von Hackeraktivität und die Eindämmung von Bedrohungen beinhaltet. Mit EDR können bereits Vorstufen von Angriffen und Hackeraktivitäten in der Phase erkannt werden, in der sich ein Angreifer im Netzwerk umsieht und ausbreitet. Um EDR jedoch effektiv zu bedienen, wird spezialisiertes Personal benötigt – und zwar rund um die Uhr, am Wochenende wie an Feiertagen. Aus diesem Grund bieten immer mehr Hersteller und Dienstleister „Managed Detection and Response“ (MDR) Dienstleistungen an, die im Auftrag der zu schützenden Unternehmen deren Netzwerke kontinuierlich auf Bedrohungen überwachen. Diese Dienstleistung ist in den meisten Fällen kostengünstiger und effektiver, als wenn Unternehmen ein eigenes Security Operations Center (SOC) für diesen Zweck aufbauen und mit eigenen Spezialisten besetzen.

Bei der Auswahl einer EDR Lösung sollten Unternehmen Wert darauflegen, dass die EDR-Lösung Angriffe nicht nur im Nachhinein erkennt, sondern bereits durch umfangreiche NextGen-Endpoint-Schutzfunktionen im Ansatz verhindert. Und wenn ein Unternehmen sich für MDR entscheidet, dann sollte der MDR-Anbieter nicht nur in der Lage sein, einen Angriff zu erkennen, sondern diesen nach Absprache mit dem betroffenen Unternehmen auch eigenständig zu stoppen.

Zusammengefasst müssen Unternehmen heute viel mehr Aufwand im Bereich der IT-Sicherheit treiben, um sich vor hochprofessionellen Angreifern zu schützen. Die traditionellen Schutzmechanismen greifen nicht mehr – da diese aber in vielen Unternehmen noch anzutreffen sind, sind die Angreifer aktuell so erfolgreich und finden täglich neue Opfer. DSGVO und Cyberrisikoversicherungen verlangen den „Stand der Technik“, der heute durch „Endpoint Detection and Response“ Lösungen plus deren effektive Bedienung definiert ist. Deshalb brauchen Unternehmen de facto „Managed Detection and Response“ Dienstleistungen, damit Geschäftsführung und IT beruhigt schlafen können. Denn es geht bei der IT-Security heute nicht mehr darum, dass diese wie in der Vergangenheit als Kostenfaktor gesehen wird – sie ermöglicht heute das Überleben von Unternehmen, die IT-Systeme einsetzen.

* Ransomware ist eine bösartige Schadsoftware, die Computer ganz sperrt oder Daten verschlüsselt. Für die Entsperrung bzw. Entschlüsselung wird oft ein Lösegeld verlangt.

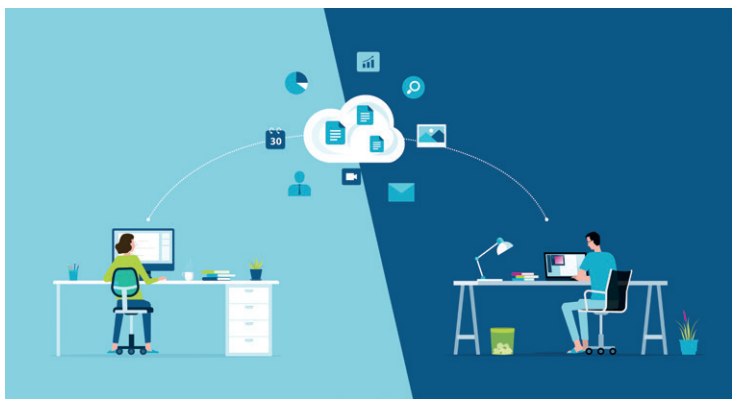
Michael Veit
Technology Evangelist
Sophos Technology Gmbh

KRZ.AKTUELL

SONDERAUSGABE November 2020

KRZ.WebOffice – Webbasierte Kollaborationsplattform

Die digitale Kommunikation ist aus unserem beruflichen Alltag nicht mehr wegzudenken. Im Zusammenhang mit unserem großen, zukunftsweisenden Projekt „KRZ.360 – Moderne IT-Lösungen aus dem KRZ-SWD“ arbeiten wir intensiv an Möglichkeiten, die den Arbeitsalltag, insbesondere das mobile Arbeiten, erleichtern sollen.



Mit KRZ.WebOffice bieten wir unseren Kunden eine zukunftssichere, webbasierte Kollaborationsplattform an, die eine echte Office-Alternative ist: Ob Tabellenkalkulation, Textverarbeitung oder Präsentation – Sie benötigen nur einen Webbrowser. Ihre Daten liegen stets sicher in unserem Dual-Rechenzentrum. Speichern, teilen und zusammenarbeiten ohne lokale Installation und mit der Sicherheit des kirchlichen Datenschutzes.

Auf einem individuell anpassbaren Dashboard sind die nachfolgenden Module von KRZ.WebOffice zusammengefasst und auf einen Blick verfügbar:

KRZ.WebOffice…

… Mail, um Nachrichten zu empfangen, versenden und zu sortieren. Auf einer Oberfläche können mehrere Nutzerkonten verwaltet werden.

… Kalender, zum Erstellen und Verwalten von Terminen

… Adressbuch, um Kontakte anzulegen, zu verwalten und versenden

… Aufgaben, zum Erstellen und Bearbeiten von Aufgaben

… Dokumente, mit den Funktionen Text, Tabelle und Präsentationen, zum Erstellen und Bearbeiten von Texten, Tabellen, Kalkulationen und Präsentationen

… Drive, um Dateien sicher in der KRZ.Cloud abzulegen, mit anderen zu teilen und gemeinsam zu bearbeiten

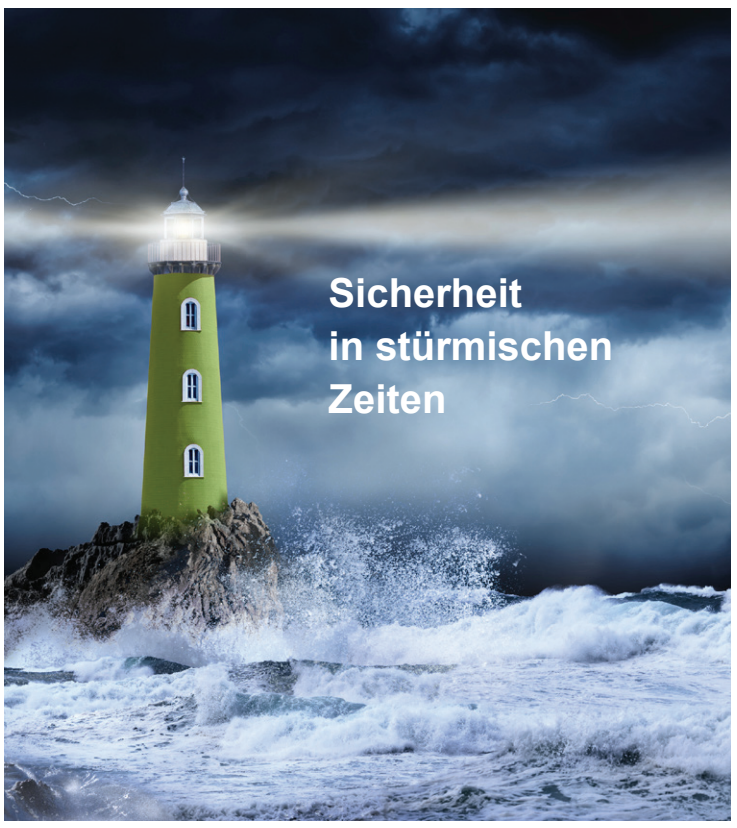
Detaillierte Informationen über KRZ.WebOffice gibt Ihnen gerne unser Vertriebsteam, E-Mail: vertrieb@krz-swd.de.

(K)RZ.Datenschutz – Verlässliche Risikoeinschätzung

Das KRZ-SWD setzt weiter auf prüfbare Qualität und wird im Jahr 2020 einen Meilenstein in punkto Sicherheit für seine Kunden setzen. Nach der klassischen Zertifizierung der Informationssicherheit (ISO 27001) und dem Datenschutz (ISO 27018 in Verbindung mit den kirchlichen Datenschutzgesetzen), sind wir auf dem Weg einer TÜViT TSI.Standard Zertifizierung nach Dual Site Level III in der Version 4.2. Jedes RZ erreicht für sich die Stufe II (von insgesamt vier). Im Verbund beider Rechenzentren erreichen wir Level III (hoher Schutzbedarf, vollständige Redundanzen kritischer Versorgungssysteme; kein „Single Point of Failure“).

Unser Rechenzentrum in Eggenstein wurde durch aufwendige Baumaßnahmen im laufenden Jahr 2020 auf den neuesten Stand gebracht. An beiden Standorten haben wir eine Personenvereinzelungsanlage installiert. Die Videoüberwachung der Sicherheitsbereiche wurde stark erweitert. Die Gebäude-Leittechnik wurde für beide Standorte vereinheitlicht und viele neue Messpunkte integriert. Daneben wurden Prozesse angepasst, die Dokumentation aller sicherheitsrelevanten Komponenten zusammengefasst und unser Sicherheitskonzept stark erweitert. Das erste TÜV Audit fand Mitte Oktober statt, ein weiteres Audit folgt Anfang Dezember.

Was bedeutet das für die KRZ-SWD Kunden?
Die sehr hohe Verfügbarkeit in Kombination mit größtmöglicher Sicherheit für die Kunden-Daten bietet jederzeit eine verlässliche Risikoeinschätzung. Zwei Hochsicherheits-Rechenzentren mit gespiegelten Sicherungsverfahren an deutschen Standorten garantieren: Das KRZ-SWD ist der richtige Partner, wenn es um zertifizierte Sicherheit und kirchenkonformen Datenschutz geht.



IMPRESSUM

Stiftung Kirchliches Rechenzentrum
Südwestdeutschland
Junkersring 10
76344 Eggenstein-Leopoldshafen
redaktion@krz-swd.de
www.krz-swd.de

Verantwortlich für den Inhalt:
Jochen Gamber, KRZ-SWD

Redaktion: Dr. Reiner Weick,
Christina Bonset, KRZ-SWD

Beiträge:
IT-Security im Wandel:
Michael Veit, Sophos Technology GmbH
KRZ.WebOffice und (K)RZ.Datenschutz:
KRZ-SWD

Gestaltung und Produktion:
Stober GmbH, Eggenstein

Bildnachweise: