Ransomware - Zusammenarbeit der KMUs mit den Strafverfolgungsbehörden

Studiengang: MAS Cyber Security

Entgegen verschiedener Medienberichte ist Ransomware nicht ausschliesslich eine Bedrohung für grosse Unternehmen. Die Angriffe richten sich gegen Firmen und Organisationen unterschiedlichster Grösse und in verschiedensten Branchen - selbst Privatpersonen bleiben davon nicht verschont.

Ausgangslage

Im Internet lauern viele und immer besser getarnte Gefahren. Aber auch die Zahl, Qualität und Vielfalt von Cyberangriffen nimmt laufend zu. Cyberkriminelle stellen für Firmen und Privatpersonen eine zunehmende und ernsthafte Bedrohung dar.
Insbesondere der Angriff mit Ransomware hat in den letzten Jahren an Bedeutung gewonnen. Gemäss Internetrecherchen sind mehr als die Hälfte der weltweit agierenden Unternehmen davon betroffen. An Kleinst- und Kleinunternehmen wird oft gar nicht gedacht, so dass sie selten bis nie in Statistiken erscheinen.
Im Unterschied zu grossen Unternehmen verfügen Kleinst- und Kleinunternehmen vermehrt über eine unzureichende IT-Sicherheit, so dass sie sich nicht ausreichend vor den Gefahren schützen können.
Während der Coronapandemie mussten viele Unternehmen rasch eine Möglichkeit zur Arbeit im Homeoffice finden, ohne dabei dem Aspekt der IT-Sicherheit gerecht zu werden, was das Risiko auf einen Angriff zusätzlich erhöhte.

Motivation

Diese Arbeit hat den Zweck den KMUs eine Hilfestellung zu bieten, die mit geringem Aufwand zu einer deutlichen Verbesserung des Eigenschutzes führen soll. Weiter soll die Zusammenarbeit im Ereignisfall zwischen den Opfern und den Strafverfolgungsbehörden verbessert werden. Für die KMUs wird ein Leitfaden erstellt, damit sie bei einem Ransomware-Angriff das Schadensausmass gering halten können. KMUs sollen motiviert werden, im Angriffsfall eine Meldung, beziehungsweise Strafanzeige einzureichen. Den Strafverfolgungsbehörden soll aufgezeigt werden, welche Präventionsmassnahmen und Unterstützungsleistungen aus Sicht der KMUs hilfreich sein könnten.

Vorgehen

Anhand einer LimeSurvey-Umfrage wurde bei ausgesuchten Verbänden und KMUs der Wissensstand zu Ransomware eingeholt. Sie soll aufzeigen, wie hoch der Anteil von Ransomware angegriffener Unternehmen ist, ob diese eine Anzeige bei den Strafverfolgungsbehörden eingereicht haben sowie welche Präventions- und Unterstützungs-Massnahmen sie sich von der Polizei wünschen. Mit einer zweiten LimeSurvey-Umfrage wurden bei den Strafverfolgungsbehörden die aktuelle Situation und Fallzahlen der Ransomware-Angriffe, die Erfahrungen in der Zusammenarbeit mit den Opfern sowie die Ausbildung der Polizeicorps erhoben. Schliesslich wurden Interviews mit einem Staatsanwalt der Staatsanwaltschaft II in Zürich, einem Cyberermittler der Stadtpolizei Zürich, einem Mitarbeiter des GovCERT sowie dem Leiter des Kompetenzzentrums Cyber Risk der Mobiliar Versicherungsgesellschaft AG geführt, um deren spezifische Sicht auf das Phänomen Ransomware zu erfahren.

Ergebnisse

Die Aussagen in den Interviews und Erkenntnisse aus den Umfragen decken sich nur teilweise mit unseren Annahmen und Erwartungen. So wurden gemäss Umfrage weniger Firmen angegriffen als angenommen. Hingegen wurde die Zusammenarbeit zwischen angegriffenen Unternehmen und den Strafverfolgungsbehörden besser bewertet als vermutet – dennoch gibt es Verbesserungspotential. Weiter erachten fast alle befragten Unternehmen die Prävention als ungenügend. Aus Sicht der Strafverfolgung müssten Betroffene konsequenter und rascher Meldung erstatten bzw. Strafanzeige einreichen.

Ausblick

Im Whitepaper für die KMUs wurden die Erkenntnisse aus den Umfragen sowie aus den Interviews zusammengefasst. Diese sollen den KMUs helfen, um einerseits ihre IT-Sicherheit mit wenig Aufwand zu verbessern und andererseits im Falle eines Angriffs durch richtiges Verhalten das Schadensausmass eindämmen. Die Thesis wird den Strafverfolgungsbehörden zur Verfügung gestellt, um ein besseres Verständnis für Opfer von Ransomware-Angriffen schaffen, das gegenseitige Vertrauen zu fördern und den Service-Public weiter zu verbessern.

Thomas Burkhalter

Daniel Schneuwly