Kommunikation bei der Incident Response

«Ich rate, nach einer Ransomware-Attacke offen zu kommunizieren»

Nach dem erfolgreichen Cyberangriff auf die IT-Infrastruktur des Erziehungsdepartements Basel-Stadt ging das Erziehungsdepartement in die Offensive. Die Öffentlichkeit wurde über den Angriff und die Publikation vertraulicher Daten im Darknet informiert. Weshalb Thomas Wenk, IT-Leiter des Erziehungsdepartements, findet, dass Organisationen viel häufiger diese Offenheit wählen sollten, erklärt er im Interview.

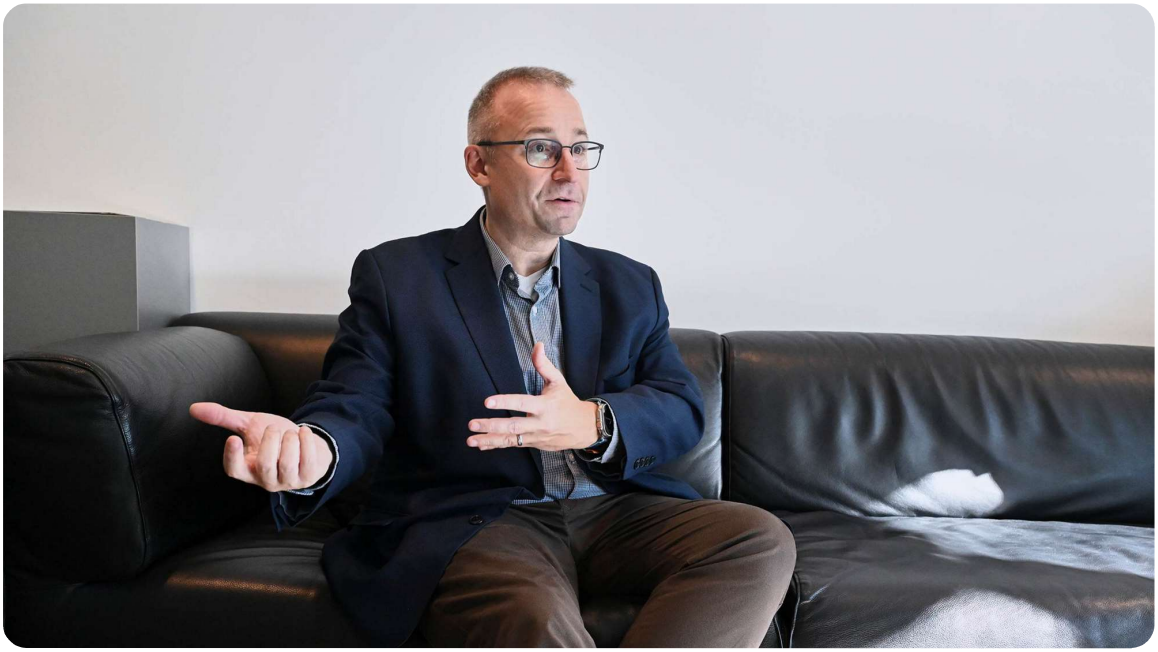
Text: Andreas Heer, Bilder: Swisscom
1. Dezember 2023

Es geschah mitten in der Umstellung auf eine neue Systemarchitektur: Anfangs 2023 gelang es Cyberkriminellen, mutmasslich via Phishing-Mail Zugriff auf die alte Infrastruktur des Erziehungsdepartements Basel-Stadt zu erhalten. Die Angreifer erbeuteten über 1 Terabyte an Daten und drohten mit der Veröffentlichung im Darknet – was anschliessend auch

passierte. Untypisch für eine Ransomware-Attacke wurden allerdings keine Daten verschlüsselt.

Das Erziehungsdepartement Basel-Stadt wählte ein unübliches Vorgehen als Reaktion auf den Vorfall. Es ging nicht auf die Lösegeldforderung ein, sondern informierte offen über den Vorfall – die betroffenen Personen, aber über die Medien auch die Öffentlichkeit.

Bei der Bewältigung des Vorfalls, der Incident Response, setzte Thomas Wenk auf das CSIRT-Team von Swisscom. Im Interview erklärt er, weshalb ihm eine offene Kommunikation wichtig ist und wie sein IT-Background, unter anderem als ehemaliger Leiter des Kompetenzzentrums digitale Ermittlungsdienste bei der Stadtpolizei Zürich, ihm bei der Bewältigung des Vorfalls half.



Thomas Wenk erklärt den Nutzen einer offenen Kommunikation in der Incident Response

Thomas Wenk, wie haben sich Ihr IT-Background und Ihre Erfahrungen in der Cybersecurity auf die Incident Response ausgewirkt?

Das hilft ungemein. Wenn man die gleiche Sprache redet und nichts erklären muss, verkürzt das die Abläufe. Das gegenseitige Verständnis und Vertrauen erleichterte uns die Aufarbeitung enorm. Zudem konnte ich als

Schnittstelle zur Geschäftsleitung des Erziehungsdepartements die Erkenntnisse in eine fürs Management verständliche Sprache übersetzen.

Andererseits war es gut, dass ich selbst nichts an der Technik mache und der Vorfall die alte Infrastruktur betraf, die wir so übernommen hatten. Dadurch hatte ich den nötigen Abstand, den es bei der Aufarbeitung eines solchen Vorfalls braucht.

Sie haben nicht nur mit dem Management kommuniziert, sondern sind mit dem Vorfall an die Öffentlichkeit gegangen. Wieso?

Wir haben natürlich vorgängig die möglichen Konsequenzen diskutiert. Für uns stand aber vom ersten Augenblick an fest, dass wir aktiv informieren werden. Auch wenn es unangenehm war, offen hinzustehen. Die Einwohnerinnen und Einwohner des Kantons erwarten von uns zu Recht eine transparente Information, gerade in einem solchen Fall.

Im Video erklärt Thomas Wenk, weshalb das Erziehungsdepartement Basel-Stadt nach der Ransomware-Attacke so offen kommuniziert hat.

Sie vertreten eine öffentliche Institution. Da dürfte der Gang an die Öffentlichkeit leichter fallen als bei einem privaten Unternehmen, das unter Umständen mit gravierenden wirtschaftlichen Folgen aufgrund des Reputationsverlustes rechnen muss. Wie schätzen Sie das ein?

Hier stellt sich für Unternehmen die Frage, wie lange sie erpressbar und die «Cash Cow» sind. Als Privatperson verstehe ich auch, wenn Firmen Lösegeld bezahlen. Das ist eine betriebswirtschaftliche Überlegung: Wenn

die Wiederherstellung verschlüsselter Daten teurer ist als das Lösegeld für den Schlüssel, ist die Antwort aus wirtschaftlicher Sicht eigentlich klar. Auch wenn dieses Unternehmen dadurch für andere Cyberkriminelle interessant wird als «zahlender Kunde».

Mit unserem Gang an die Öffentlichkeit haben wir diesen Mechanismus durchbrochen. Dadurch waren wir nicht mehr erpressbar. Natürlich haben wir vorgängig die nötigen internen Stellen informiert.

Viele Unternehmen, gerade in sensiblen Branchen, schätzen aber das Risiko und den Reputationsverlust bei einer offenen Kommunikation offenbar als zu hoch ein.

Das ist eine einfache Rechnung: Wie hoch ist die Wahrscheinlichkeit, dass der Vorfall geheim bleibt? Und wenn ihn jemand anderer aufdeckt, wie lange dauert es, bis ich mich von diesem Schaden erholt habe? Solche Überlegungen müssen sich Firmen anstellen. Es ist durchaus wahrscheinlich, dass bereits Fragen kommen, wenn zum Beispiel die Mitarbeitenden plötzlich das Passwort wechseln müssen. Ich rate deshalb, offen zu kommunizieren.

Cybersecurity ist auch Teamwork. Das heisst, Unternehmen sind auf Informationen von anderen Organisationen über die kriminellen Akteure angewiesen. Inwiefern hilft es für dieses Teamwork, nach einem Vorfall offen zu kommunizieren?

Wir arbeiten mit verschiedenen Gremien des Bundes zusammen wie dem NCSC. Dort haben wir auch transparent kommuniziert. Ich hoffe, mit der offenen Kommunikation können wir einer Organisation helfen, die in einer ähnlichen Situation steckt oder in eine solche kommt.

Ich habe schon bei meiner früheren Stelle bei der Stadtpolizei Zürich gesagt: Der Mensch verliert nicht gerne. Wir müssen also lernen, zu verlieren. Wir müssen lernen, vor die Leute hinzustehen und sagen, dass es uns getroffen hat. Wir müssen auch über die Misserfolge reden und sagen,

was passiert ist. Damit können wir anderen helfen, dass es ihnen nicht auch passiert. Deshalb müssten mehr Firmen offen kommunizieren.

Über Thomas Wenk

Seit April 2021 leitet der Basler Thomas Wenk die Abteilung Digitalisierung und Informatik des Erziehungsdepartements Basel-Stadt. Zuvor stand er während mehreren Jahren dem Kompetenzzentrum Digitale Ermittlungsdienste der Stadtpolizei Zürich vor, wo er sich sein Team unter anderem mit digitaler Forensik, Cybercrime und Internet-/Darknet-Ermittlungen beschäftigte. Als IT-Leiter war der Ökonom Thomas Wenk bereits früher tätig, als er die Zentralen Informatikdienste des Kantons Basel-Landschaft leitete.

Keine Inhalte verpassen

Erhalten Sie regelmässig spannende Artikel, Whitepaper und Event-Hinweise zu aktuellen IT-Themen für Ihr Unternehmen.

Anmeldung

swisscom

Verwandte Artikel

Whitepaper

Ransomware: Funktionsweise und Schutz

Erfahren Sie im Whitepaper mehr über Ransomware-Angriffe und wie Sie sich davor schützen können.

→ Mehr erfahren

Threat Detection & Response

Threat Detection & Response

Mit Threat Detection & Response (TDR) wehren Sie Cyberangriffe auf Ihr Unternehmen ab. Profitieren Sie von einer...

→ Mehr erfahren

swisscom