„Es geht um das **Vertrauen** der Kunden“

Vor rund zehn Monaten wurde die Kisters AG Opfer eines Hackerangriffs, ließ sich jedoch nicht erpressen. Ein Rückblick mit Vorstand **Klaus Kisters**.

VON FRITZ WILHELM

Klaus Kisters: „Die Kunden im Unklaren zu lassen, kam für uns nicht in Frage“

Quelle: Kisters AG

E&M: Herr Kisters, warum haben Sie sich entschieden, den Hackerangriff auf Ihr Unternehmen öffentlich zu machen?

Kisters: Es geht vor allem um Vertrauen – in erster Linie um das Vertrauen der Kunden. Uns war klar, dass es einige Zeit dauern wird, bis wir wieder Software produzieren können. Darüber die Kunden im Unklaren zu lassen und irgendwelche Ausreden wie ‚technische Probleme‘ vorzuschieben und floskelhaft um etwas Geduld zu bitten, kam für uns nicht in Frage.

E&M: Wie haben Ihre Kunden reagiert?

Kisters: Sehr positiv. Wir haben von unseren Kunden sehr viel Zuspruch und Unterstützung bekommen. Viele haben uns auch in unserer Entscheidung bestärkt, uns nicht erpressen zu lassen.

„Bis heute sind keinerlei Kundendaten im Darknet aufgetaucht“

E&M: Sind denn Daten aufgetaucht?

Kisters: Nein, den Ermittlern zufolge sind bis heute keinerlei Kundendaten im Darknet aufgetaucht und kein Kunde hat bis heute überhaupt eine Kompromittierung aufgrund des Vorfalls bei Kisters festgestellt.

E&M: Welchen Schaden haben Sie dann davongetragen?

Kisters: Die Hacker haben tatsächlich Daten abgezogen, aber vor allem Verschlüsselungen gestartet. Dabei haben unsere Virenscanner erkannt, dass ungewöhnliche Prozesse ablaufen, und ein paar von ihnen noch rechtzeitig stoppen können. Aber bei einigen Systemen haben wir das Wettrennen mit den Kriminellen dann doch leider knapp verloren.

E&M: Das heißt, Sie waren sich der Gefahren bewusst und waren vorbereitet?

Kisters: Wir waren vorbereitet. Wir gehören ja selbst nicht zur kritischen Infrastruktur, arbeiten aber für Kritis-Unternehmen. Wir halten uns an die Grundschutzempfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik; d. Red.). Wir haben ein TÜV-zertifiziertes Rechenzentrum. Wir selbst und auch unsere Kunden überprüfen uns immer wieder mit Penetration Tests und weiteren Sicherheitsüberprüfungen. Wir führen regelmäßig Awareness-Übungen mit unseren Mitarbeitern durch. Wir sind seit 2017 ISO 27001-zertifiziert und haben seit 2016 einen hauptamtlichen CISO (Chief Information Security Officer; d. Red.), der alle Systeme und deren Sicherheitsanforderungen kennt und die entsprechenden Maßnahmen koordiniert. Und Gutachter haben uns im Nachhinein bescheinigt, dass alle unsere Verbindungen zu den Systemen unserer Kunden State of the Art waren.

> „Es ist keine gute Option, einer Lösegeldforderung nachzukommen“

„Wir waren vorbereitet“

E&M: Und trotzdem haben es die Hacker geschafft einzudringen.

Kisters: Leider ja. Für uns stellte sich dies jedoch immer als eine abstrakte Gefahr dar. Und wie so oft im Leben, ist man zuversichtlich, dass es einen selbst nicht trifft. Erfahrene Ermittler gehen aber mittlerweile davon aus, dass heutzutage nicht mehr die Frage ist, ob man gehackt wird, sondern wann es passieren wird.

E&M: Haben Sie vorher Angriffe bemerkt?

Kisters: Ja, wie jedes andere Unternehmen registrieren wir ständig Angriffe, praktisch minütlich, und konnten sie bis auf das eine Mal im vergangenen November immer abwehren.

E&M: Wissen Sie, mit welchen Kriminellen Sie es zu tun hatten?

Kisters: Ja, das war die Conti-Gruppe. Mittlerweile hat sie sich wohl aufgelöst. Die hatte ‚Ransomware as a Service‘ quasi als ‚Geschäftsmodell‘.

E&M: ... das Sie aber nicht unterstützt haben. Hatten Sie schon zu einem früheren Zeitpunkt festgelegt, im Falle eines Falles kein Lösegeld zu zahlen?

Kisters: Das war nicht in Stein gemeißelt. Aber bei näherer Betrachtung wird schnell klar, dass es keine gute Option ist, einer Lösegeldforderung nachzukommen. Denn wer einmal zahlt, erweist sich als lohnendes Zielobjekt. Gleichzeitig muss man sich immer vor Augen führen, dass man ja einen Vertrag mit Kriminellen schließt und das Risiko besteht, dass sie sich nicht an die Vereinbarungen halten. Das kommt laut den Ermittlern aber tatsächlich selten vor. In der Regel werden die Schlüssel wohl herausgegeben und die Erpressten bekommen gegebenenfalls sogar noch Hilfestellung, wenn die Entschlüsselung nicht sofort funktioniert. Es handelt sich ja um ein Geschäftsmodell. Was mit gestohlenen Daten und Informationen passiert, ist eine andere Frage.

E&M: Wie hoch war die Lösegeldforderung in Ihrem Fall?

Kisters: Wir können dazu keine detaillierten Angaben machen. Es ist wohl üblich, dass Erpresser etwa fünf bis zehn Prozent des Jahresumsatzes als Forderung aufrufen. Dann ist man schnell bei einem siebenstelligen Betrag.

E&M: Aber der Schaden insgesamt ist sicherlich höher.

Kisters: Auf jeden Fall. Der kann sich alles in allem auf einen achtstelligen Betrag aufsummieren, auch wenn man kein Lösegeld zahlt. Denn man hat im Nachgang erhebliche Investitionen, um den Vorfall aufzuarbeiten, die eigene Produktion wieder in Gang zu bringen, neue Sicherheitsmaßnahmen zu etablieren, um hier nur einige unserer Schadenspositionen zu nennen. Wir haben beispielsweise alle Systeme vollständig neu aufgebaut. Das heißt, wir haben jeweils die neueste Firmware der Hersteller installiert und nicht die Backups, die wir selbstverständlich hatten, für das Wiederaufspielen der Software genutzt. Wir haben alle aktiven Netzwerkkomponenten, Firewalls und Betriebssysteme erneuert.

„Wir haben alle Systeme neu aufgebaut“

E&M: Sind dann Backups nach einem solchen Angriff eigentlich wertlos?

Kisters: Nein. Für einen Insel-Notbetrieb kann man die Backups nutzen. Man kann auch Daten, etwa Dokumente, von den Backups zurückspielen, wenn man sie mehrfach auf Viren untersucht hat. Aber die Software, also die Anwendungsprogramme, sollte man komplett neu aufsetzen. Die Ermittler haben dringend dazu geraten, da auch Backups von Hackern kompromittiert werden können. Zusätzlich haben unsere mehr als 300 Entwickler ihren Quellcode der letzten drei Monate im Vier-Augen-Prinzip geprüft, um das Risiko einer Supply-Chain-Attacke durch unsere Software möglichst auszuschließen.

E&M: Muss man sich auch neue Hardware zulegen?

Kisters: Nicht unbedingt. Es geht vor allem um die Software und die Hintertüren, die von Hackern dort eingesetzt werden können. Deshalb haben wir vorsorglich rund tausend Workstations in unseren Büros weltweit komplett neu installiert. Es ist wichtig, all diese Maßnahmen transparent zu machen. Schließlich geht es um das Vertrauen der Kunden. Deshalb haben wir diesen Wiederaufbau auch gutachterlich begleiten lassen und jeden Schritt dokumentiert.

E&M: Muss man dafür den genauen Hergang des Angriffs und das exakte Einfallstor kennen?

Kisters: In 95 Prozent aller Fälle lasse sich nicht genau sagen, durch welche Tür die Hacker eingedrungen sind, haben uns die Forensiker erklärt. Das ist bislang auch bei uns der Fall. Es sind aber auch noch nicht alle Untersuchungen abgeschlossen.

E&M: Haben Sie einen Verdacht?

Kisters: Bei allen möglichen Anwendungsprogrammen treten immer wieder Sicherheitslücken zutage. Ich möchte aber nicht weiter spekulieren.

E&M: Wie war Ihre Zusammenarbeit mit den Ermittlern?

Kisters: Die war sehr angenehm, vertrauensvoll und professionell. Wir haben intensiv mit der ZAC (Zentrale Ansprechstelle für Cybercrime der Polizei; d. Red.) hier in NRW zusammengearbeitet und tun das noch immer. Wichtig ist: Das sind Spezialisten vor Ort, die bei uns wenige Stunden, nachdem wir den Angriff entdeckt hatten, vor der Tür standen. Es nutzt ja nichts, wenn irgendwo zentral in Deutschland Leute sitzen, mit denen man per Telefon oder Teams kommuniziert. Man hat sich ja gerade aus Sicherheitsgründen komplett vom Internet abgekoppelt. Außerdem haben wir Berater hinzugezogen, die beim BSI als qualifizierte APT-Response-Dienstleister (Advanced Persistent Threat; d. Red.) gelistet sind. Auch mit ihnen war die Zusammenarbeit sehr gut.

E&M: Was sind für Sie die Lessons Learned aus dem Vorfall?

Kisters: Es hat sich bewährt, einen CISO und ein eigenes IT-Administrationsteam für den Wiederaufbau im Haus zu haben sowie eng mit den Spezialisten der ZAC und des APT-Teams zusammenzuarbeiten. Genauso, offen zu kommunizieren. Gleichzeitig muss man aufpassen, wie weit man dabei geht. Wenn man detaillierte Informationen darüber gibt, was man macht, gibt man gleichzeitig preis, was man nicht macht, was wieder Kriminelle auf den Plan rufen könnte. Das ist natürlich ein Spagat. E&M

Angriff vor Mitternacht

Kurz vor Mitternacht des 10. November 2021 haben Mitarbeiter des permanent überwachten Rechenzentrums der Kisters-Gruppe den Beginn von Verschlüsselungsprozessen festgestellt. Auf Basis des Sicherheitsleitfadens des BSI haben die Verantwortlichen entschieden, das gesamte Unternehmen mit allen Systemen weltweit unverzüglich vom Internet zu trennen und auch interne Verbindungen zu unterbrechen. Kurz nach Mitternacht wurden die Polizei und die Zentrale Ansprechstelle Cybercrime (ZAC) der Polizei in NRW verständigt. Am frühen Morgen des 11. November haben Spezialisten der ZAC und des APT-Teams mit der forensischen Arbeit begonnen. Parallel gab es einen intensiven Austausch mit der Bundesnetzagentur und dem BSI. Am 16. November gab das BSI eine Sicherheitsmitteilung nach dem sogenannten Traffic Light Protocol (TLP) an die Betreiber kritischer Infrastrukturen heraus.
Nach wenigen Tagen konnte Kisters den Support für seine Kunden über verschiedene Kommunikationskanäle der Mitarbeiter wieder aufnehmen. Nach mehreren Sieben-Tage-Arbeitswochen hatte die Gruppe bis Weihnachten 2021 die vollständige Kommunikationsfähigkeit hergestellt. Und im März 2022 teilte das Unternehmen mit, die Softwareproduktion wieder aufgenommen zu haben.