Der Mittelstand im Visier von Hackern

Was sich anhört wie ein Krimi war für Dirk Sieverding und sein Team ein Albtraum über mehrere Wochen

Der Mittelstand mutiert zum Lieblingsopfer von Hackern – jedes dritte Unternehmen wurde bereits Ziel eines Angriffs. Die einzige Abwehr: Die IT-Infrastruktur professionell und konsequent sichern. Wie das geht und was bei einem Cyber-Angriff zu tun ist, hat Dirk Sieverding beim zwei.7 Unternehmer-Talk im Dialog mit Karsten Wulf erklärt, bei denen Entrepreneurs regelmäßig über Themen sprechen, die Mittelständlern unter den Nägeln brennen. Er ist CEO der Remmers Gruppe, die selbst Opfer einer Ransomware-Attacke geworden ist.

Mehrere Millionen Euro hat das Unternehmen aus Löningen seit der digitalen Attacke vor 5 Monaten verloren. An die Erpresser, externe IT-Expert*innen, den Wiederaufbau der Informationsinfrastruktur. Und noch immer läuft in der IT nicht alles rund.

Mit einem Klick lag plötzlich die komplette digitale Infrastruktur des mittelständischen Familienunternehmens, das bauchemische Produkte sowie Holzfarben und -lacke herstellt, lahm. Drucker, Telefone, Computer – und vor allem die Produktion standen still. Hunderte Mitarbeitende wurden nach Hause geschickt, Kund*innen wurden informiert. Erst als eine Lösegeldforderung in Form einer Textdatei im System gefunden wurde, war klar: Wir sind Opfer eines Cyberangriffs.

Verschlüsselungssoftware legt komplette Infrastruktur lahm

Hacker konnten durch eine Sicherheitslücke im verwendeten Betriebssystem von Microsoft alle Passwörter auslesen und so eine Verschlüsselungssoftware ins Unternehmenssystem spielen. Bei diesen so genannten Zero Day Exploit Attacks missbrauchen Cyberkriminelle öffentlich bekannt gewordene Programm-Schwachstellen bevor die Entwickler Zeit hatten, sie zu beheben. Frei nach dem Motto: first come, first serve. Oder aus Kriminellen-Sicht: Der Schnellste kann abkassieren.

Für die Verhandlung mit den Erpressern hat sich der Geschäftsführer Dirk Sieverding professionelle Hilfe geholt von jemandem, der es können muss erzählte er Karsten Wulf und den 35 aufmerksamen Teilnehmern: ein Experte, der schon mal auf der anderen Seite stand. Wie er unterstützen geschulte IT-Expert*innen Unternehmen, die ins Fadenkreuz von Internetkriminellen geraten. Denn von den Behörden erhielt Sieverding keine Unterstützung.

Verhandlung mit Unterstützung von externem Dienstleister

Trotzdem blieb nur eins, um wieder Herr des IT-Netzwerkes zu werden: das Lösegeld bezahlen – in Bitcoin über das Darknet. Als Antwort erhielt er ein Passwort, das die Datenverschlüsselung aufhebt. Drei Wochen später waren die Unternehmenssysteme wieder frei.

Die Attacke hat die Remmers Gruppe einen mittleren siebenstelligen Betrag gekostet: für Betriebsausfall, externe Dienstleister, das Lösegeld und den Wiederaufbau der IT. Durchschnittlich müssen Unternehmen dafür 47 Millionen US-Dollar aufbringen, um so eine Attacke zu beheben.

Wie sich Unternehmen vor Cyber-Angriff schützen können

Der Fall Remmers Gruppe beweist: Mittelständische Unternehmer*innen mit einer Das-passiert-nur-den-Großen-Einstellung, gehen ein großes Risiko ein. Längst ist der Mittelstand eins der

Lieblingsopfer von Hackern, weil sie häufig Cybersicherheit nicht ernst nehmen. Deshalb waren die Teilnehmer des zwei.7 Unternehmertalks auch dankbar, für die Informationen aus erster Hand.

Der beste Schutz vor Cyber-Attacken ist eine sichere IT-Infrastruktur. Mit diesen Maßnahmen können Sie Ihr Unternehmen schützen:

1. **Professionelle IT-Sicherheitsprüfung**
   Ein IT-Sicherheitsaudit von Expert*innen durchführen lassen. Expert*innen prüfen unter anderem mit einem simulierten einen Angriff Ihre IT gestützten Geschäftsprozesse auf mögliche Risiken. Der staatlich geförderte Check bringt neben Sicherheitslücken auch Optimierungs- und Effizienzmöglichkeiten hervor. Die Kosten liegen im vierstelligen Bereich.

2. **Zwei-Faktor-Authentifizierung**
   Für die Anmeldung in Unternehmenssystemen wird die herkömmliche Authentifizierung durch Benutzernamen und Passwort um einen weiteren Faktor ergänzt – zum Beispiel einen Fingerabdruck oder einen Code, der ans Smartphone gesendet wird. So können sich Unbefugte auch dann keinen Zugang zu Ihrem Netzwerk verschaffen, wenn sie das Passwort kennen.

3. **Ein IT-Sicherheitsbeauftragter**
   Der IT-Expert*in schafft, pflegt und überwacht Systeme und Prozesse, die die Datensicherheit in Ihrem Unternehmen sichern. Er prüft Risiken und sensibilisiert Mitarbeiter*innen für einen sicheren Umgang mit Unternehmensdaten.

4. **Intelligente Cloudstrategie nutzen**
   So werden die Daten nicht zentral an einem Ort gespeichert und sind so im Falle eines Angriffs oder einer Systemstörung verfügbar.

Unternehmer-Talk: Austausch und Expertise für den Mittelstand

Dirk Sieverding teilte seine Erfahrungen jüngst mit anderen Mittelständlern im zwei.7 Unternehmer-talk „Cybercrime im Mittelstand“. In der Veranstaltungsreihe laden wir regelmäßig Entrepreneurs mit Themen ein, die Unternehmer*innen aus dem Mittelstand unter den Nägeln brennen: vom Recruiting, Unternehmensnachfolge, Geschäftsmodellen der Zukunft bis zur Strategieentwicklung.

Sie wollen dabei sein?
Wir laden Sie gerne zu unserer nächsten Veranstaltung ein. Schreiben Sie uns einfach eine E-Mail an julia.heitling@zweipunkt7.com.