Wer nicht möchte, dass sein Server gehackt wird, muss sich mit „Defense in Depth“ und „Zero-Trust“ auseinandersetzen

„Die Gefahr ist nicht größer als zuvor“

Seit dem Ukraine-Krieg steht **Cybersicherheit** bei vielen Unternehmen wieder ganz oben auf der Tagesordnung. Die IT-Experten und Unternehmer Dr. Stefan Leinenbach und Dr. Philipp Walter glauben jedoch nicht daran, dass sich die Bedrohungslage für die Wirtschaft nun drastisch verschärft.

Herr Leinenbach, wurden Sie schon mal gehackt?

Leinenbach: Beinahe. Es gab zuvor tatsächlich eine Cyberattacke auf den öffentlichen Personennahverkehr. Meine Tochter nutzt als Schülerin eine Monatskarte, was eine entsprechende Bescheinigung, dass sie Schülerin ist, voraussetzt. Deshalb habe ich diese Bescheinigung an eine ordentliche Mailadresse des ÖPNV-Anbieters geschickt. Meine Mail wurde dort von den Hackern abgefangen. Eine Antwort kam zurück: Vielen Dank, aber leider fehlen noch Angaben, ich möge bitte angehängtes Word-Dokument ausfüllen. Unsere IT-Sicherheit im Haus hat das Word-Dokument jedoch vorsorglich automatisch entfernt – wir nutzen kein Microsoft Office mehr im Haus, weil deren Dokumente mit sogenannten Makro-Viren versehen sein können. Ich wäre jedoch darauf hereingefallen, weil die Hacker eine schlüssige Kommunikation fingiert haben. Möglicherweise hat man mich sogar gezielt als Geschäftsführer eines IT-Unternehmens ausgesucht.

„Sobald ein Server mit dem Internet verbunden ist, beginnen Attacken“

Herr Walter, wie bereiten Sie sich angesichts von Cyberkriminalität, auch möglicher russischer Cyberattacken, vor?

Walter: Wir haben unsere Strategie mit Beginn des Krieges nicht grundlegend geändert. Denn auch jene Cyberangriffe werden sich von Art und Umfang nicht groß von den alltäglichen Angriffen unterscheiden. Sobald ein Server mit dem Internet verbunden ist, beginnen die Attacken – meist eher harmlose Verbindungsversuche, automatisierte Scans ohne besonderes Engagement, die schwache Passwörter und andere Nachlässigkeiten abklopfen. Wird dabei schon eine Schwachstelle entdeckt, werden solche kompromittierten Systeme meist „auf Vorrat“ für weitere Attacken gehalten. Dies macht etwa 99 Prozent aller Angriffe auf Computersysteme aus. Anschließend können aber aufwendigere manuelle Angriffe folgen, die sich durch neue Ertragsmodelle für Cyberkriminelle auf Basis von Kryptowährungen lohnen, zum Beispiel mithilfe von Ransomware. Also: das Erpressen von Systembetreibern, indem ihr System gehackt und die Daten verschlüsselt werden und nur nach Zahlung eines Betrages X in Kryptowährung wieder entschlüsselt werden.

Leinenbach: Das einzig Positive im Augenblick ist, dass IT-Risiken wieder in den Fokus rücken. Sie werden wieder bewusster wahrgenommen, obwohl sie Stand jetzt nicht signifikant größer sind als zuvor. Deshalb spricht man uns verstärkt an seit Kriegsbeginn. Das Thema IT-Sicherheit in Unternehmen sollte allerdings ein Dauerthema sein.

Wie sehen die Strukturen hinter den Angriffen aus?

Walter: Es sind kriminelle Wirtschaftssysteme, die dahinterstecken. Die Schwachstellen-Scanner und Passwort-Abfischer sind sozusagen die erste Kolonne, erbeutete Zugänge werden auf Schwarzmarktplätzen verkauft, wo sie dann für kriminelle Zwecke weiterverwendet werden. Das ist die Bedrohungslage, die wir schon vor dem Ukraine-Krieg gesehen haben – seither macht dieser Krieg in der Hinsicht jedoch nicht viel aus. Es gibt Hinweise auf russische Akteure wie Killnet, aber wir sehen keine besonders ausgeklügelten Attacken. Ein sogenannter „state actor“, also ein Angreifer im Dienst eines Staates, würde Systeme auf andere, subtilere Art kompromittieren.

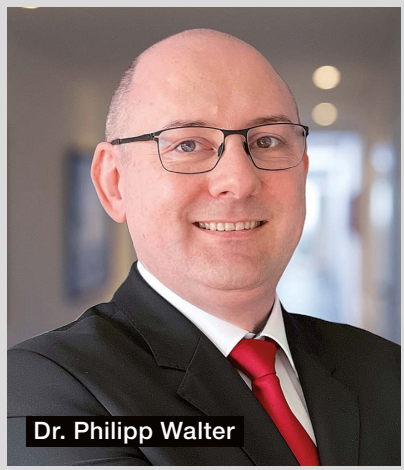
FOTOS: INFOSERVE (2) — BECKERBREDEL / INFOSERVE

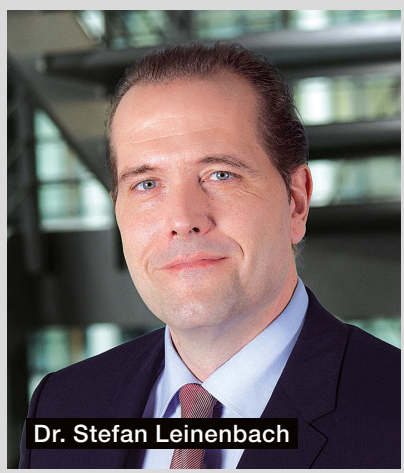
Prominent durch die Medien ging der Fall Kaspersky, ein russischer Hersteller von Antivirensoftware. Kann man dem Unternehmen und dem Programm, das viele auch zu Hause installiert haben, vertrauen?
Walter: Es besteht Unklarheit. Bisher gibt es keinen Indikator, dass das Programm dazu genutzt wurde, um Angriffe zu unterstützen. Aber es gibt auch keine Klarheit mehr darüber, dass es nicht dafür benutzt werden könnte. Sie operieren nun mal aus Russland heraus, einem Land, das wir nicht als Rechtsstaat ansehen können. Macht der Staat Druck, kann es beispielsweise zu einer Supply-Chain-Attacke kommen. Dabei wird Schadsoftware über eine bewusst in dem Produkt platzierte Schwachstelle beim Verbraucher eingeschleust. Geschieht das bei Antivirensoftware, ist das besonders kritisch, weil diese höhere Privilegien als andere Programme besitzt, um den gesamten Rechner auf Schadsoftware überwachen zu können.

Leinenbach: Es gibt Unternehmen, die hier umstellen, weil ihnen das Risiko einer potenziellen Schwachstelle zu groß ist. Vorsicht ist sicher angeraten. Wir müssen unterscheiden zwischen privaten und geschäftlichen Nutzern dieser Software. Auch bei privaten Nutzern müssen wir schauen, handelt es sich um eine an anderer Stelle exponierte Person in der Politik oder Wirtschaft? Generell wollen wir nicht von dieser Software abraten, verstehen aber die Skepsis, die dazu führt, dass manche auf andere Anbieter umstellen möchten.

ZUR PERSON

Die Diplom-Informatiker **Dr. Stefan Leinenbach** und **Dr. Philipp Walter** leiten als Geschäftsführer und IT-Leiter das System- und IT-Sicherheitsunternehmen Infoserve.


Dr. Philipp Walter


Dr. Stefan Leinenbach

Die Bedrohungslage wird unabhängig von Russland größer. Welche Strategien verfolgen Unternehmen heute, um sich abzusichern?
Walter: Es gibt unterschiedliche Strömungen: Früher hieß es Firewall, Proxy und Antivirenschutz reicht, und es gibt sicher noch Firmen, die so arbeiten. Heute aber heißt es beispielsweise „Defense in Depth", also mehrstufige Verteidigung, eigentlich ein militärischer Begriff. Normalerweise bewegt sich ein Hacker von Schwachstelle zu Schwachstelle. Mit der „Defense in Depth" innerhalb der IT wird der Angreifer statt nur einmal am Perimeter immer wieder am Fortkommen bis hinein in den Kern des Systems gehindert. Oder es herrscht eine „Zero-Trust-Policy", ebenfalls ein aktueller Begriff. Hierbei vertrauen die Systeme sozusagen niemandem, das heißt, es gibt kein internes Netzwerk mit nur einer einzigen starken Authentifizierung zur Absicherung des Zugriffs von außen mehr. Stattdessen

„Schwachstelle Nummer eins ist immer noch der Mensch"

ist jedes einzelne System eine Insel und dementsprechend stark geschützt, zum Beispiel mit einem Hardware-Schlüssel, den man in den USB-Port des Rechners schiebt, sich damit zusätzlich authentifiziert und anmeldet.

Leinenbach: Die Schwachstelle Nummer eins ist immer noch der Mensch, zum Beispiel durch ein schwaches Passwort, das er vergibt. Über Software-Schwachstellen in ein System einzubrechen ist einfacher, wenn es keine Zwei-Faktor-Authentifizierung gibt. Sprich, ein zusätzliches, dynamisch erzeugtes Kennwort oder ein vom Computer unabhängiges Hardware-Teil. Wir kennen das zum Beispiel beim Onlinebanking: dazu brauchen wir heute nicht nur einen Rechner, sondern auch die Bankkarte und ein Stück Hardware, das Karten-Lesegerät. Dennoch bleiben die Hacker auch hier kreativ.

Walter: Ja, beispielsweise durch Sim-Swap. Das heißt, Kriminellen kann es gelingen, den Support eines Telekommunikationsanbieters davon zu überzeugen, dass das Smartphone eines Kunden gestohlen wurde. Man möge doch bitte eine neue Sim-Karte verschicken, natürlich nicht an die hinterlegte Adresse, sondern an die des Angreifers. So kann auch die Telefonauthentifizierung ausgehebelt werden.

Leinenbach: Daran sehen wir: Die Technik muss immer mitwachsen, den Faktor Mensch kann man relativ einfach überprüfen.

Inwiefern überprüfen?
Leinenbach: Wir werden hin und wieder von Unternehmen aufgefordert, sie selbst zu Testzwecken zu hacken. Das müssen wir sogar regelmäßig tun, denn IT-Sicherheit ist kein Zustand, sondern ein kontinuierlicher Prozess. Indem wir dies regelmäßig tun, decken wir diese menschlichen Schwachstellen wie schwache Passwörter auf. Finden wir diese, können wir aktiv werden und sie schließen. Eine ständige Sensibilisierung ist bei diesem Thema einfach notwendig, um am Ball zu bleiben, denn natürlich stellt sich bei vielen Unternehmen schnell Routine ein.

Sind die Unternehmen denn heute bereit dafür, dieses Thema zur Chefsache zu machen statt es an die IT zu delegieren?
Walter: Die Bedrohungslage ist niemandem verborgen geblieben. Mittlerweile ist die Sicherheit von Unternehmen so weit oben im Risikomanagement aufgehängt, dass es der Bedeutung der IT als kritischem Produktionsfaktor auch gerecht wird.

Interview: Falk Enderle