Schutz auf allen Ebenen

Für kritische Infrastrukturen nimmt die Bedrohung durch Cyber-Angriffe zu, die Anforderungen an die Sicherheit steigen. IT- und Serviceprovider prego services hat ein modulares Sicherheitskonzept für die Versorgungsbranche entwickelt. Ein Bestandteil ist ein modernes Security Operations Center (SOC).

Nach einer kurzen Einführung öffnet Peter Schreieck, Teamleiter Communications & Network bei der prego services GmbH, eine speziell gesicherte Tür und wir dürfen die Sicherheitszentrale betreten. Mit seinen großen Flachbildschirmen an der Stirnwand erinnert der Raum an eine Leitstelle, an den Schreibtischen sitzen die Mitarbeitenden konzentriert vor ihren Bildschirmen. „Wir überwachen hier die Aktivitäten in den Netzwerken unserer Kunden", beschreibt der Verantwortliche die Funktion des Security Operations Center (SOC). „Hier klassifizieren und bearbeiten wir sicherheitsrelevante Meldungen und ergreifen Maßnahmen, falls erforderlich", ergänzt er.

Das SOC sei nur ein Element eines modernen modularen Sicherheitskonzepts, erklärt Schreieck, der seit fast 20 Jahren bei prego services arbeitet. Am Anfang steht die „Härtung" der Hardware. So sichert prego services für Kunden beispielsweise neu installierte Geräte in der Konfiguration speziell ab, bevor sie ins Netzwerk integriert werden – so wird neben dem Virenscanner eine zusätzliche Schutzinstanz geschaffen. „Selbstverständlich kümmert sich unser Team auch darum, dass die Software stets auf aktuellem Stand bleibt", erklärt Schreieck.

Secure by Design

In einer zweiten Stufe geht es um eine sichere IT-Infrastruktur. „Secure by Design ist unsere Kernphilosophie, die wir gemeinsam mit unseren Kunden aktiv umsetzen", bekräftigt der Security-Spezialist. Je besser das Gesamtsystem und die Einzelkomponenten dabei aufeinander abgestimmt würden, desto höher die Sicherheit. Eine ausgeklügelte Firewall sei dabei Dreh- und Angelpunkt. „Eine moderne Firewall ist heutzutage extrem komplex und dynamisch", erläutert Schreieck. Denn ungewollte Zugriffe müssen verhindert werden, ohne den reibungslosen Datenaustausch im Tagesgeschäft zu behindern. Die steigende Zahl mobiler Arbeitsplätze sei dabei eine besondere Herausforderung

Das Team von Schreieck empfiehlt beim Aufbau einer resilienten IT-Infrastruktur zudem das Schaffen von Redundanzen und die Einrichtung von beispielsweise demilitarisierten Zonen (DMZ). „Ähnlich wie im Mittelalter Burgen durch mehrere Burgwälle, Wassergraben und Wachtürme gesichert wurden, arbeiten wir mit einer Kombination von unterschiedlichen Schutzmaßnahmen."

Security Monitoring

Im SOC wird die dritte Stufe des Sicherheitskonzepts umgesetzt: Die Echtzeit-Überwachung der Kunden-Netzwerke. Um die enormen Mengen an Informationen über deren Zustände und aufgetretene Ereignisse zu bewältigen, nutzt prego services automatisierte Prozesse. Doch Peter Schreieck relativiert: „Wir setzen künstliche Intelligenz in bestimmten Bereichen ein. Es gibt aber auch Netzwerkanomalien oder Meldungen, die die Systeme nicht abschließend beurteilen können. Nur gut ausgebildete Security-Spezialisten können solche Vorfälle und Zusammenhänge analysieren, einordnen und bewerten – letztendlich sorgen Menschen für Sicherheit."

Jeden Tag mindestens ein Angriff

Schreieck zeigt auf einen der Bildschirme an der Wand. Dort blinkt eine Warnmeldung, der Mitarbeiter ist bereits in Kontakt mit dem Kunden. „Das war eine False Positive Meldung", erklärt er. „Es hat sich herausgestellt, dass der Kunde Wartungsarbeiten durchgeführt hat, ohne uns zu informieren." Neben diesen leicht aufzuklärenden Missverständnissen erlebt das SOC aber täglich ernsthafte Angriffe.

Eine weitere Erfahrung: Malware und Ransomware werden nicht nur immer häufiger in Umlauf gebracht, sondern auch qualitativ besser. „Unsere Malwareerkennung bietet einen umfangreichen Schutz. Trotzdem kann es natürlich vorkommen, dass gefälschte E-Mails mit Dateianhängen durchdringen. Hier kommt es darauf an, die Belegschaft regelmäßig zu schulen und über aktuelle Gefahren zu informieren", betont der Sicherheitsexperte.

Sicherheitsgemeinschaft

Ganz wichtig ist Peter Schreieck die enge Kooperation mit dem BSI sowie die Mitarbeit in der Allianz für Cybersicherheit und bei UP KRITIS, einer öffentlich-privaten Kooperation zwischen Betreibern kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen. „Durch den engen Informationsaustausch sind unsere Security-Spezialisten immer auf dem aktuellen Stand und wissen sehr konkret, welche Sicherheitslücken aktuell mit welcher Schadsoftware angegriffen werden", erklärt Schreieck.

Steigende Anforderungen an KRITIS-Unternehmen

Das ist auch notwendig, denn die Angreifer werden immer besser und aggressiver. Allein im Jahr 2021 ermittelte das BSI über 144 Millionen neue Schadsoftware-Varianten. Das illegale Geschäftstreiben richtete nach Berechnungen des Branchenverbands Bitkom bereits im Vorjahr Schäden von 223 Milliarden Euro an. Seit dem Beginn des Ukrainekriegs dürfte sich die Bedrohung weiter erhöht haben. Daher ist die Sensibilität für Cyber-Sicherheit in der Politik enorm gewachsen. Bundesinnenministerin Nancy Faeser hat erst kürzlich eine Änderung des Grundgesetzes vorgeschlagen, um das BSI mit weiteren Kompetenzen auszustatten.

Gelänge ein großangelegter Angriff auf die (zunehmend digitalisierte) Versorgungsinfrastruktur, wären die Folgen tatsächlich unabsehbar. Aus diesem Grund gelten für Unternehmen der kritischen Infrastruktur besonders hohe gesetzliche Anforderungen. Betreiber von IT-Netzen innerhalb der kritischen Infrastruktur müssen ab einer bestimmten Unternehmensgröße im Kontakt mit dem BSI stehen, die Umsetzung von IT-Sicherheit nach aktuellem Stand der Technik nachweisen sowie IT-Störungen und -Beeinträchtigungen melden. Das neue IT-Sicherheitsgesetz 2.0 schafft noch weitergehende Pflichten. So müssen KRITIS-Unternehmen unter anderem Systeme zur Angriffserkennung nutzen und nachweisen. Es steht zu erwarten, dass zunehmend auch kleinere Unternehmen diese Anforderungen erfüllen müssen. Peter Schreieck begrüßt diese Entwicklung. „Kriminellen Angreifern ist die Unternehmensgröße ohnehin egal, sie suchen einfach schlecht geschützte Netzwerke", kommentiert er lakonisch.

Gleichzeitig sind IT Security-Spezialisten Mangelware und die meisten Dienstleister sind ausgebucht. Wer jetzt noch keine professionelle Cyber-Sicherheit eingeführt hat, steht in Angriffsfall mit dem Rücken zur Wand. „Stellen Sie sich vor, Ihr Haus brennt und alle Feuerwehreinheiten im Umkreis sind in anderen Einsätzen gebunden", mahnt Peter Schreieck. „Dann kann Ihnen niemand helfen, das müssen Sie einfach wissen."

Auf einem Bildschirm an der Wand des SOC leuchtet eine neue Warnung auf. Zeit also, die Spezialisten konzentriert weiter arbeiten zu lassen. (pq)

www.prego-services.de

Die permanente Überwachung der Kunden-Netzwerke im Security Operation Center (SOC) ist eine Komponente der Dienstleistungen, die prego services anbietet, um kritische Infrastrukturen vor Cyber-Angriffen zu schützen. (Foto: prego services GmbH)