Keine Chance für Angreifer

In der virtuellen Welt gilt wie in der realen Welt: Die Gefahr eines Anschlags ist dort am größten, wo am meisten zerstört werden kann. Stark frequentierte Bereiche werden schnell zur Zielscheibe. Unternehmen, die ihr Rechenzentrum anderen zur Verfügung stellen, müssen mit der passenden Lösung für besonderen Schutz sorgen.

Die Büroräume werden über Nacht abgeschlossen, damit sind die unternehmenskritischen Unterlagen in Sicherheit. Doch wer das Firmennetz nicht ausreichend schützt, kann darauf getrost verzichten. Angriffe auf Netzwerke häufen sich und richten immer größer werdenden Schaden an.

Eine einfache Firewall hält den aggressiven Attacken längst nicht mehr stand. Hacker greifen auf ungesicherte Privatcomputer zu, koppeln sie zu regelrechten Botnetz-Armeen und legen so ganze Unternehmensnetze lahm.

Eine unzureichend geschützte IT-Landschaft öffnet Hackern Tür und Tor, sei es zur Spionage, um ein Unternehmen gezielt zu schädigen oder um sich auf andere Weise einen Wettbewerbsvorteil zu verschaffen. Die Angriffsszenarien ändern sich nahezu täglich. Daher ist eine ausdifferenzierte Schutzlösung notwendig.

Frühzeitig handeln

Leider reagieren viele Unternehmen erst, nachdem ihr Netzwerk angegriffen und möglicherweise bereits geschädigt wurde. Dann rufen sie einen Fachmann auf dem Gebiet der IT-Security zu Hilfe, in der Hoffnung, dass der schnell den passenden „Rettungsring“ zuwirft. Dieser besteht aus einer zügigen Analyse des Netzwerks und der Auswahl einer passenden Lösung. „Gerade Unternehmen, die selbst Dienstleistungen im Netzwerkbereich anbieten, sind in Gefahr“, erklärt Matthias Waschke, Vertriebsleiter für Service Provider bei der circular Informationssysteme GmbH.

Das trifft auch auf den Rechenzentrumsbetreiber und Hosting-Anbieter aixit GmbH zu. Das Unternehmen stellt ein Rechenzentrum mit hochverfügbarer Infrastruktur bereit und vermietet die entsprechende Hardware an seine Kunden. Es ist auf Sicherheitssysteme angewiesen, damit es die virtuellen Zugänge des Rechenzentrums überwachen kann.

Kürzlich kam ein Kunde aus der Online-Gaming-Branche auf den Hosting-Anbieter zu. Die Mitarbeiter hatten regelmäßige Angriffe auf das Firmennetz bemerkt und fürchteten, ihr Unternehmen könne Schaden nehmen.

Holger Grauer, CTO bei aixit, sagt: „Hinter einer Schädigung des Unternehmensnetzwerks steht heute nicht selten das Bestreben, sich gegenüber einem Konkurrenten einen Wettbewerbsvorteil zu verschaffen. Es werden eigens Strategien entwickelt, um gezielt Server von Mitbewerbern anzugreifen.“

Individuell passendes Sicherheitskonzept

Dieses Vorgehen war zuerst im Online-Gaming-Sektor verbreitet, wo Spieler die Rechner von Gegnern angriffen, um sie auszuschalten.

Holger Grauer hat es jedoch schon in vielen Bereichen beobachtet. Er schildert einen Fall von zwei konkurrierenden Unternehmen, die um die Platzierung von Werbung im Internet stritten. „Werbefläche ist entsprechend teuer. Wenn einer der beiden Kontrahenten dafür sorgt, dass das Netzwerk des anderen lahmgelegt wird, kann dieser plötzlich gar keine Werbung mehr schalten. Sobald aber nur noch ein Interessent übrig ist, verbilligt sich der Preis für die Online-Werbung minütlich radikal.“

Ein echter Angriff zeigt, wie gut sensible Kundendaten geschützt sind.

Die Rechenzentren von Hosting-Anbietern müssen absolut ausfallsicher sein.

Um sich vor solchen Methoden zu schützen, benötigen Unternehmen ein gut durchdachtes Sicherheitskonzept. Eine passende Lösung zu finden, fällt den meisten Unternehmen schwer. Nahezu unüberschaubar ist der Markt an Sicherheitslösungen geworden. So war auch aixit auf Sicherheitsspezialisten angewiesen, die sie bei der Entscheidung für eine entsprechende Lösung beraten. Nach der Anfrage des Kunden aus der Online-Gaming-Branche startete der Hosting-Anbieter daher eine Ausschreibung.

Gute Pakete – schlechte Pakete

Im Rahmen eines internen Auswahlverfahrens fiel die Entscheidung zu Gunsten von circular. Dieser Anbieter stellte ein auf der Software von Arbor Networks basierendes Konzept vor.

Holger Grauer berichtet: „Uns war es wichtig, circular als erfahrenen Partner mit im Boot zu haben. Dieser unterstützt uns dabei, die passende Lösung zu finden, kennt sie gut und hilft uns aktiv bei der Installation, Konfiguration und Implementierung. Im Notfall können wir die Experten sogar am Wochenende oder spät abends erreichen."

Der Sicherheitsspezialist prüfte die konkreten Anforderungen des Online-Gaming-Kunden. „Im Vordergrund stand dabei immer die Frage: Wie trägt das Konzept zu einer höheren Sicherheit des Unternehmensnetzwerks bei? Für die gewählte Lösung sprach, dass sie Angriffe auf Netzwerk- und Applikationsebene erkennt und behebt", erklärt Matthias Waschke.

Das Sicherheitssystem analysiert ständig den kompletten Netzwerkverkehr, erkennt Anomalien und gibt im Ernstfall Warnungen ab. Sie decken so schadhafte Komponenten auf und entfernen sie. Vereinfacht dargestellt, leitet das System „gute" Pakete weiter und sortiert „schlechte" aus. Dabei wird der reguläre Datenverkehr nicht unterbrochen.

Da das System „lernfähig" ist, kann es auch neuartige Würmer oder Viren entdecken. Für den Kunden bedeutet das: Das Unternehmensnetz ist vor Systemausfällen und kriminellen Aktivitäten geschützt und die Anwendungen sind auch während eines Angriffs verfügbar. Aus diesem Grund hat sich das Online-Gaming-Unternehmen dazu entschlossen, die Sicherheitslösung als Managed Service in vollem Umfang einzusetzen.

Sofort wieder verfügbar

Bereits während der sechswöchigen Testphase hat sich das Sicherheitssystem bewährt. Schon nach vier Tagen wurde das Netzwerk tatsächlich angegriffen. Und in weniger als 30 Sekunden war das System wieder erreichbar. „Selbstverständlich könnte man einen solchen Angriff auch simulieren, aber nichts überzeugt Unternehmensleiter so, wie bei einem echten Angriff die Leistung des Sicherheitssystems zu sehen", sagt aixit-CTO Holger Grauer.

Mittlerweile hat der Gaming-Anbieter sämtliche Türen für Unbefugte abgeschlossen – auch die virtuellen. Das Projekt hat Holger Grauer überzeugt: „Der Einsatz des Systems erfordert keine Änderung der kompletten Netzwerkstruktur. Daher nutzen wir die Lösung jetzt auch selbst." *[rm]*

Gefahrenpotenzial für ungesicherte Netzwerke

- Diebstahl von unternehmenskritischen Informationen
- Industriespionage
- Daten und Programme können manipuliert werden.
- Das System kann vollständig ausfallen.
- Im Angriffszeitraum ist das Unternehmen nicht erreichbar.
- Wettbewerbsnachteile gegenüber konkurrierenden Unternehmen
- Der Super-GAU: Rufschädigung des Unternehmens und hohe finanzielle Verluste