Adieu, Corporate Networks?

Digitalisierung erfordert ein – teilweise radikales – Umdenken für die IT-Security. Ist die Perimetersicherheit für den Schutz interner Ressourcen noch zeitgemäß? Die explodierende Zahl von Smart Devices und die Cloud lassen Zweifel aufkommen.

TEXT —— Roger Homrich

Noch vor wenigen Jahren war die Angst groß, mobile Mitarbeiter zu integrieren, ihnen den Zugriff auf das Intranet zu gewähren. Wie sollten sich die Risiken managen lassen, wenn Hunderte verschiedene Smartphones, Laptops oder Tablets auf Daten und Anwendungen in der so hoch gesicherten Trutzburg zugreifen? Die IT-Security schützt das Unternehmensnetzwerk mit allen Mitteln gegen Angriffe und die eigenen Mitarbeiter öffnen mit ihren mobilen Endgeräten Tür und Tor für Hacker. „Bring your own Device" war für die meisten IT-Verantwortlichen neben der Cloud ein rotes Tuch schlechthin. Heute sind mobiles Arbeiten und Cloud Computing Standard.

Lässt sich das bisherige Verteidigungskonzept damit noch aufrechterhalten? Das Perimetersicherheitsmodell funktionierte gut, solange alle Angestellten ausschließlich in Gebäuden eines Unternehmens arbeiteten und alles, was unterwegs war, außen vor blieb. Mit dem Aufkommen einer mobilen Belegschaft, der zunehmenden Vielfalt verwendeter Geräte und der verstärkten Nutzung Cloud-basierter Dienste sind jedoch zusätzliche Angriffsflächen entstanden.

„Die geänderten Rahmenbedingungen erfordern es, sich über bestehende Sicherheitskonzepte Gedanken zu machen. Die bisherige Taktik, ein Corporate Network aufzubauen, das wie eine Burg mit Gräben, Mauern und Zugbrücken verteidigt wird, funktioniert nicht mehr so richtig", warnt Thomas Tschersich, Leiter Internal Security & Cyber Defense der Telekom.

RAUS AUS DEN EIGENEN VIER WÄNDEN

Was hat sich geändert? Bisher haben Unternehmen die IT innerhalb ihres Corporate Network betrieben – ob in eigenen oder in Rechenzentren von IT-Dienstleistern. Alles spielte sich zu Hause ab, in den eigenen vier Wänden. Wer durch die Tür reinwollte, wurde kontrolliert, brauchte ein Visum oder wurde als Einwohner registriert und bekam dauerhafte oder temporäre – zum Beispiel projektbezogene – Aufenthaltserlaubnis. Wer keinen gültigen Pass vorzeigen konnte, den ließen die Firewalls nicht durch.

Doch das funktioniert immer weniger. Denn schlaue Angreifer versuchen Schlupflöcher im Unternehmensnetzwerk zu finden und treiben dann – oft unentdeckt – ihr Unwesen. „Der Aufwand, ein solch geschlossenes Netzwerk sicher zu machen, ist in den vergangenen Jahren enorm gestiegen. Unternehmen können das kaum mehr allein bewältigen, da die Zahl und Intelligenz der Angreifer exponentiell angestiegen sind", sagt Tschersich. Und provokativ setzt der Securityexperte noch einen drauf: „Man muss sich schon fragen, ob aus sicherheitstechnischer Überlegung ein Corporate Network überhaupt noch zeitgemäß ist."

Aufschrei. Steht nicht gerade ein Unternehmensnetzwerk für Sicherheit? Das sei nicht ganz falsch, so Tschersich, aber Unternehmen müssten sich der Tatsache stellen, dass IT nichts mehr mit dem zu tun hat, wofür IT noch vor zehn Jahren stand: dem Betrieb proprietärer Software im eigenen Rechenzentrum, auf die nur eigene Mitarbeiter zugreifen durften. „Heute nutzen immer mehr Unternehmen Standardsoftware in der Cloud. Public-Cloud-Angebote lassen sich aber nicht im eigenen Corporate Network betreiben. Die Software liegt irgendwo zusammen mit den Daten bei einem Provider. Weit außerhalb der eigenen Burg", erklärt Tschersich.

Wer als Mitarbeiter diese Software nutzt, verlässt automatisch das Corporate Network. Entweder geht es aus dem Büro in die Cloud oder von außen mit dem Smartphone über eine Tür ins Netzwerk rein und an anderer Stelle wieder von innen durch eine andere Tür aus dem Netzwerk raus. „Warum sollten wir daher den Schutz nicht zum Endgerät legen? Dann sparen wir uns den ganzen Aufwand für das Unternehmensnetzwerk", bringt es Tschersich auf den Punkt.

IOT VERÄNDERT SECURITYKONZEPTE

Es sind nicht nur die klassischen mobilen Endgeräte und die Cloud, die das bisherige Modell des Corporate Networks auf den Kopf stellen. In viel größerer Stückzahl wird jedes vernetzte Gerät im Internet der Dinge neue Securityansätze erfordern. Auch das vernetzte Auto. Sie alle senden Daten in das Intranet und die Cloud. Sie müssen erst ins Netzwerk rein und wieder raus. Der Aufwand für die Abschirmung des Unternehmensnetzwerks wird dadurch weiter ansteigen.

Auch Edge Computing bringt neue Herausforderungen mit sich: Entsprechend verlagert sich die Analyse von Daten an den Rand des Netzwerks oder sogar nach draußen. Und damit wird es kompliziert. Ein einzelnes Smart Device kann eine verschlüsselte VPN-Verbindung ins Firmennetzwerk erzeugen. Für komplexere Systeme müssen Unternehmen aber spezialisierte Router, Routing Switches, integrierte Zugangsgeräte, Multiplexer und SD-WAN-Lösungen nutzen und managen. Die Komplexität des eigenen Netzwerks steigt enorm an.

Wie also kann ein Unternehmen den Schutz nach wie vor gewährleisten, obwohl sich die Grenzen zwischen Privat- und Unternehmensnetz verschoben haben? Gibt es Alternativen? „Die gibt es“, verspricht der Chef der internen Telekom Security. „Endgeräte lassen sich mit Securitysoftware schützen.“ Was anscheinend nicht allen bekannt ist, denn laut einer Umfrage von IDC zählen in Deutschland unzureichend oder mangelhaft gesicherte Endgeräte zu den top-Sicherheitsrisiken in den Unternehmen. „Die Securityverantwortlichen müssen hier noch einiges tun. Lösungen gibt es aber auf dem Markt. Und natürlich ist es wichtig, die Endgeräte aktiv zu managen. Dazu gehört es, Updates zentral aufzuspielen oder Schatten-IT in Form von Apps zu verhindern. Aber das ist nicht neu, sondern muss einfach konsequent umgesetzt werden“, betont Tschersich.

BEI GOOGLE ZÄHLT NUR DAS ENDGERÄT

Ein prominentes Beispiel für den Abschied vom Corporate Network ist Google. Der Zugriff auf die interne IT hängt ausschließlich von den Anmeldeinformationen des Geräts und des Benutzers ab. Der Netzwerkstandort eines Benutzers ist weniger wichtig – sei es ein Unternehmensstandort, ein Heimnetzwerk, ein Hotel oder ein Café. Der gesamte Zugriff auf Unternehmensressourcen ist vollständig authentifiziert, autorisiert und verschlüsselt, basierend auf dem Gerätestatus und den Benutzerdaten.

Google verwendet das Konzept des „Managed Device“. Das Unternehmen beschafft jedes Gerät und verwaltet es aktiv. Nur diese Geräte können auf Unternehmensanwendungen zugreifen. Ein Geräteverfolgungs- und -beschaffungsprozess, der sich um eine Gerätebestandsdatenbank dreht, ist ein Eckpfeiler dieses Modells. Alle verwalteten Geräte müssen eindeutig identifiziert werden. Sie verweisen dafür auf einen Datensatz in der Device Inventory Database, einer Datenbank für die Geräteinventarisierung. Eine Möglichkeit der eindeutigen Identifizierung ist ein gerätespezifisches Zertifikat. Um ein Zertifikat zu erhalten, muss ein Gerät in der Datenbank vorhanden und zertifiziert sein. Die Zertifikate liegen in einem Zertifikatsspeicher. Nach der Installation wird das Zertifikat in der gesamten Kommunikation mit den Unternehmensdiensten verwendet.

„Das Modell Google hat einen weiteren Vorteil für die Securityabteilungen“, erklärt Tschersich und weiß aus eigener Erfahrung, wovon er spricht. „Wir Sicherheitsabteilungen kommen damit ein Stück weit raus aus unserer Verbieterrolle und übernehmen stattdessen eine aktiv gestaltende Rolle in der Digitalisierung.“

Thomas.Tschersich@telekom.de
www.t-systems.de/loesungen/security

Die Rechnung, ihr Corporate Network wie eine Burg mit Gräben, Mauern und Zugbrücken zu sichern, geht für viele Unternehmen nicht mehr auf.

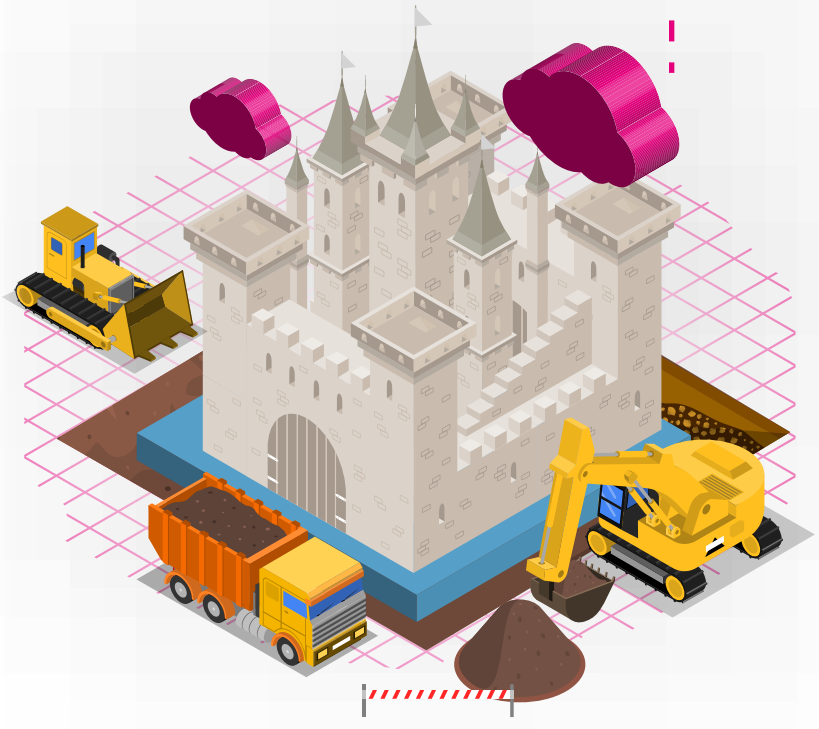

Illustration: freepik.com