Dirk Fox

Perimetersicherheit

Begriff

Mit *Perimeter* wird die Grenzlinie eines Geländes oder Bereichs bezeichnet. Der *Perimeterschutz* konzentriert sich auf die Absicherung dieser Grenzlinie. Das erfolgt – wie schon im Mittelalter – meist durch Umfriedung mit Mauern, Zäunen und Wachpersonal, heute auch zunehmend durch Videoüberwachungsanlagen. Ziel des Perimeterschutzes ist, nur an wenigen zentralen Stellen einen kontrollierten Zugang zu einem Gelände oder Gebäude zu erlauben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) widmet dem Perimeterschutz von Rechenzentrumsgebäuden in den IT-Grundschutzkatalogen eine eigene Maßnahme (M 1.55 [1]). Danach sollen Perimeterschutz-Maßnahmen – abhängig vom Schutzbedarf – sowohl vor unbeabsichtigtem als auch beabsichtigtem bis hin zu gewaltsamem Überwinden der Grundstücksgrenze durch Unbefugte schützen.

Ergänzend zu den oben genannten Maßnahmen listet das BSI darin Personen- und Fahrzeugidentifikation, Videogegensprechanlagen, Schleusen, Zutrittskontrolleinheiten, Geländebeleuchtung und Detektionssensorik mit Alarmierungseinrichtungen auf.

Unter *Perimetersicherheit* versteht man entsprechende Schutzmaßnahmen für die IT-Infrastruktur. Als Perimeter werden dabei die Grenzen des Unternehmensnetzes verstanden – in der Regel also die Verbindung des Intranet mit dem Internet.

Schutzmaßnahmen

„Klassische" Maßnahmen zur Gewährleistung von Perimetersicherheit sind vor allem Firewalls. Mit ihnen soll verhindert werden, dass Unberechtigte von außen Verbindungen ins interne Netz aufbauen können. Sie werden heute zumeist von zahlreichen weiteren Maßnahmen flankiert:

- In einem von der Firewall abgetrennten Netzsegment, auch DMZ (Demilitarisierte Zone) genannt, werden Systeme betrieben, die vom Internet aus zugänglich sein sollen (wie z. B. Webserver und E-Mail-Server). Über definierte Firewall-Regeln können diese wiederum Verbindungen mit ausgewählten Systemen im internen Netz aufbauen (z. B. einer Datenbank zur Annahme von Bestellungen aus einem Online-Shop auf dem Webserver).
- Direkte Internet-Verbindungen von Rechnern aus dem internen Netz werden häufig über einen Proxy-(Stellvertreter-)Server geleitet, auf dem z. B. Schadsoftware auf Internet-Seiten herausgefiltert werden kann. Auch die Sperrung von Webseiten anhand von Verbots- (Blacklist) oder Erlaubnislisten (Whitelist) ist so möglich, sogar die Analyse von SSL-Verbindungen.
- Mit Spam- und Virenfiltern werden E-Mail-Anhänge auf gefährliche Schadsoftware untersucht und ggf. gelöscht.
- Um die eindeutigen IP-Adressen der Endsysteme nicht preiszugeben, erfolgt an der Firewall in der Regel eine Network Address Translation (NAT, Ersetzung der IP-Adresse), sodass alle Internet-Zugriffe aus dem internen Netz immer mit derselben Absenderadresse (der Firewall) erscheinen.

Schließlich können Angriffserkennungssysteme Alarmierungen auslösen und schnelle Reaktionen ermöglichen.

Grenzen

Die Perimetersicherheit unterliegt zunächst ähnlichen Beschränkungen wie der Perimeterschutz: Sie kann zwar Eindringversuche abwehren; gelingt es einem Angreifer jedoch, ins interne Netz zu gelangen, ist die Schutzwirkung ausgehebelt. Dies kann – ähnlich dem Trojanischen Pferd in der griechischen Mythologie – z. B. durch das Einschleusen eines mit Schadsoftware infizierten Datenträgers gelingen.

Perimetersicherheit ist außerdem anfällig für „Denial of Service"-Angriffe[1]: Wird der durch die Firewall kontrollierte Zugangspunkt zum internen Netz durch Verbindungswünsche überlastet, kann die Verbindung des internen zum äußeren Netz abbrechen. Firewalls sind damit ein „Single Point of Failure": wer sie außer Gefecht setzt, unterbricht alle Kommunikationsverbindungen.

Schließlich kann die Perimetersicherheit (ebenso wie ein Perimeterschutz) durch versteckte Hintertüren konterkariert werden: Bohrt jemand Löcher in den Schutzwall, indem er z.B. das interne Netz über einen WLAN-Hotspot oder einen DSL-Anschluss als Bypass mit dem Internet verbindet, können Angreifer darüber den Firewall-Zugang umgehen.

Aber auch aktuelle Entwicklungen der Informationstechnik bedrohen die Perimetersicherheit:

- Schlecht geschützte und unverschlüsselte Web-basierte Zugänge zum internen E-Mail-System bohren ein Loch in den Schutzwall.
- Smartphones, die mit internen Systemen synchronisiert und außerhalb des Unternehmens mit unzulänglichen Schutzmechanismen genutzt werden, können unterwünschten Datenabfluss begünstigen.
- Verschlüsselte Verbindungen und E-Mails können nur sehr eingeschränkt an der Firewall kontrolliert werden und ermöglichen so ggf. „Huckepack"-Angriffe.
- Verschlüsselte VPN-Verbindungen für Außendienstmitarbeiter oder Home-Offices öffnen einen weiteren Zugang ins interne Netz, der wirksam vor Missbrauch geschützt werden muss.
- „Inside-Out"-Angriffe können von innen ein Loch in die Firewall bohren und eigentlich unzulässige Protokolle und Verbindungen in ein zugelassenes Protokoll (wie http) einpacken und die Filter der Firewall damit „durchtunneln".

Perimetersicherheit allein kann daher moderne IT-Infrastrukturen nicht mehr wirksam vor Angriffen schützen.

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): M 1.55 Perimeterschutz, Maßnahmenkatalog IT-Grundschutz, Stand 2009 https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m01/m01055.html

1 Siehe Kelm/Möller, *Distributed Denial of Service-Angriffe (DDoS)*, DuD 5/2000.