ZUERST ANS ENDE DENKEN

Clients besser absichern mit
Advanced Endpoint Security

Experten schätzen, dass zwei Drittel der erfolgreichen Cyberangriffe über den Anwender erfolgen – sprich über dessen Endgeräte. Neben klassischen Clients wie Desktop und Notebook gehören dazu auch mobile Geräte wie Tablet oder Smartphone. Angesichts der immer höheren Qualität der Angriffe stoßen traditionelle Schutzmaßnahmen wie Firewall und Antiviren-Programme an ihre Grenzen. Um Endpunkte zu schützen, ist eine Advanced Endpoint Protection notwendig.

EINFALLSTOR ENDPUNKT

Vor allem über die Endpunkte und den Missbrauch von Benutzerrechten erlangen Angreifer Zugriff auf kritische Daten – bei etlichen der bekannt gewordenen Sicherheitsvorfälle lag genau dort die Schwachstelle. Und diese potenziellen Einfallstore wachsen im Zeitalter der zunehmenden Vernetzung im Internet of Things und von Industrie 4.0 exponentiell an. Entscheidende Argumente für Unternehmen, ihren Fokus deutlich stärker als bisher auf den Endpunkt zu legen. Dabei ist die Frage nach dem Wie nicht leicht zu beantworten: Einerseits wird der Herstellermarkt mit neuen Anbietern und Lösungen immer unübersichtlicher, andererseits entstehen durch neue Angebote für Detektion und Reaktion überhaupt erst völlig neue Marktsegmente. Dabei sollten Security-Lösungen vor allem eins: im Hintergrund ganz unbemerkt von den Anwendern für die notwendige Sicherheit sorgen.

DER MIX IST ENTSCHEIDEND

Unverzichtbare Basis für die Endgerätesicherheit bilden etablierte Sicherheitsmaßnahmen – also das Härten und Patchen von Betriebssystemen und Applikationen sowie deren sicherer Betrieb. Kurz- bis mittelfristig bleibt es zudem notwendig, auf die klassische Endpoint-Security mit signaturbasierten und heuristischen Analysen zu setzen. Um jedoch auch gezielte Angriffe aufzudecken und deren Auswirkungen einzudämmen, sollte sich eine Advanced Endpoint Protection aus weiteren Technologien zusammensetzen, unter anderem:

- Exploit Mitigation
- Behaviour Monitoring
- Application Control
- Containment

Je nach individuellen Sicherheitsanforderungen eines Unternehmens empfiehlt sich ein Mix der Lösungen: Denn während sich beispielsweise Application Control im Produktionsumfeld mit statischen Systemen eignet, wäre es für die Office-IT mit ihren kurzen Patchzyklen zu aufwendig. Die Einführung von Behaviour Monitoring ist sinnvoll, wenn bereits ein Security Operation Center (SOC) inklusive Know-how von Security-Analysten besteht. Falls nicht, eignen sich Exploit-Mitigation-Lösungen, da die Software bekannte Kerntechniken eines Angriffs auf einem Client verhindert und die Auswirkungen von Exploits begrenzt.

BERATUNG – BESCHAFFUNG – INTEGRATION

Auf Basis von Proof of Concepts erstellt Computacenter gemeinsam mit seinen Kunden einen Kriterienkatalog für den größtmöglichen Schutz der eingesetzten Endgeräte. Dabei profitieren Unternehmen sowohl von den langjährigen Partnerschaften, die Computacenter mit allen führenden Security-Herstellern pflegt, als auch von der kontinuierlichen Analyse und Bewertung neuer Security-Anbieter und -Lösungen am Markt. Mit unserem umfassenden Security-Portfolio bieten wir für alle Gerätetypen und Sicherheitsebenen die passenden Lösungen.

DIGITAL Trust. Mastering business security

Computacenter

Computacenter AG & Co. oHG
Europaring 34–40, 50170 Kerpen

computacenter.de
+49 (0)2273 5970