Endpoint Security: Wenn Endgeräte zum Risiko werden

23.06.2026, 16:40 | IT, New Media & Software

Pressemitteilung von: *NetWyl Informatik GmbH*

Mobile Geräte erhöhen die Flexibilität - und die Angriffsfläche. Erfahren Sie, warum Endpoint Security heute entscheidend für den Schutz moderner Unternehmens-IT ist.

Luzern im Juni 2026: Laptops, Smartphones, Tablets und hybride Arbeitsplätze haben den modernen Unternehmensalltag grundlegend verändert. Mitarbeitende greifen heute von unterschiedlichsten Standorten auf sensible Daten, Cloud-Dienste und Unternehmensnetzwerke zu. Gleichzeitig steigt damit die Zahl potenzieller Angriffspunkte massiv an. Während Unternehmen ihre Prozesse digitalisieren und flexibler gestalten, nutzen Cyberkriminelle genau diese Entwicklung gezielt aus.

Besonders betroffen sind Unternehmen, deren Mitarbeitende regelmässig mobil arbeiten oder private sowie geschäftliche Geräte parallel verwenden. Denn jeder einzelne Endpunkt - ob Notebook im Homeoffice oder Smartphone unterwegs - kann zum Einfallstor für Angriffe werden. Genau deshalb gewinnt das Thema Endpoint Security zunehmend an strategischer Bedeutung.

Sicherheitsfachleute beobachten dabei eine deutliche Veränderung der Bedrohungslage: Früher konzentrierten sich Angriffe primär auf zentrale Serverstrukturen. Heute richten sie sich gezielt gegen Endgeräte, weil dort Sicherheitslücken, menschliche Fehler oder unzureichende Schutzmechanismen besonders häufig auftreten.

Immer mehr Unternehmen berichten von ähnlichen Herausforderungen: unbekannte Geräte im Netzwerk, fehlende Transparenz über Sicherheitsstände oder Unsicherheit darüber, welche Systeme tatsächlich geschützt sind. Besonders kritisch wird die Situation dort, wo veraltete Geräte, unkontrollierte Softwareinstallationen oder fehlende Updates auf zunehmenden Zeitdruck im Arbeitsalltag treffen. Erfahren Sie mehr darüber: https://www.netwyl-informatik.ch/leistungen/endpoint-security/ .

Der Arbeitsplatz hat keinen festen Standort mehr

Die klassische Unternehmensinfrastruktur mit klar abgegrenzten Büroarbeitsplätzen existiert in vielen Branchen kaum noch. Mitarbeitende arbeiten unterwegs, im Homeoffice oder an wechselnden Standorten. Dateien werden in Cloud-Umgebungen gespeichert, Projekte kollaborativ bearbeitet und Unternehmensdaten auf unterschiedlichsten Geräten verarbeitet.

Damit verändert sich auch die Rolle moderner Sicherheitskonzepte. Sicherheit muss heute dort funktionieren, wo sich Mitarbeitende tatsächlich befinden - unabhängig vom Standort oder Endgerät.

Gerade dieser Wandel stellt viele Unternehmen vor neue Herausforderungen. Denn traditionelle Schutzmechanismen wie Firewalls oder zentrale Netzwerküberwachung greifen nur begrenzt, wenn Geräte ausserhalb des Unternehmensnetzwerks genutzt werden.

Endpoint Security verfolgt deshalb einen anderen Ansatz: Nicht nur das Netzwerk wird geschützt, sondern jedes einzelne Gerät selbst. Sicherheitsfunktionen arbeiten direkt auf den Endpunkten und erkennen Bedrohungen unabhängig davon, wo sich ein Gerät gerade befindet.

Warum Endgeräte heute besonders gefährdet sind
Cyberkriminelle konzentrieren sich zunehmend auf Endgeräte, weil diese oft die schwächste Stelle in der Sicherheitsarchitektur darstellen. Ein einzelnes kompromittiertes Notebook genügt unter Umständen, um Zugriff auf zentrale Systeme oder sensible Unternehmensdaten zu erhalten.
Besonders problematisch ist dabei die Kombination verschiedener Faktoren: fehlende Updates, unsichere WLAN-Verbindungen, private Nutzung geschäftlicher Geräte oder unkontrollierte Softwareinstallationen.

Viele Angriffe beginnen deshalb nicht mit hochkomplexen technischen Schwachstellen, sondern mit alltäglichen Situationen. Eine manipulierte Datei, eine schädliche Browser-Erweiterung oder ein gefälschter Login reichen häufig aus, um Schadsoftware auf einem Gerät zu installieren.

Ein anonymisierter IT-Verantwortlicher eines mittelständischen Unternehmens beschreibt die Situation so:
"Wir gingen lange davon aus, dass unsere zentrale Infrastruktur ausreichend geschützt sei. Erst nach einem Vorfall wurde sichtbar, wie viele Risiken tatsächlich direkt auf den Endgeräten entstehen."

Solche Erfahrungen zeigen ein Problem, das Sicherheitsfachleute zunehmend beschäftigt: Unternehmen verlieren oft den Überblick darüber, welche Geräte im Einsatz sind, welchen Sicherheitsstatus sie besitzen und welche Risiken daraus entstehen.

Die Folgen reichen weit über technische Probleme hinaus
Ein erfolgreicher Angriff auf ein Endgerät bleibt selten auf einen einzelnen Arbeitsplatz beschränkt. Moderne Schadsoftware bewegt sich gezielt innerhalb von Netzwerken weiter, verschlüsselt Daten oder versucht, administrative Zugänge zu übernehmen.

Dadurch entstehen Risiken, die weit über technische Störungen hinausgehen. Produktionsunterbrüche, Kommunikationsprobleme, finanzielle Schäden oder Reputationsverluste können innerhalb kurzer Zeit erhebliche Auswirkungen haben.

Besonders kritisch wird dies bei mobilen Arbeitsplätzen oder dezentralen Teams. Wenn zentrale Datenbestände kompromittiert oder Systeme verschlüsselt werden, droht im schlimmsten Fall ein vollständiger Betriebsausfall.

Hinzu kommt die Gefahr von Datenverlust. Geschäftsdokumente, Kundendaten oder interne Informationen können bei erfolgreichen Angriffen nicht nur beschädigt, sondern auch gestohlen oder veröffentlicht werden. Gerade im B2B-Umfeld entstehen daraus erhebliche wirtschaftliche und rechtliche Risiken.

Experten beobachten deshalb einen klaren Trend: Unternehmen investieren verstärkt in Sicherheitslösungen, die Bedrohungen bereits auf Endgeräten erkennen und stoppen, bevor sich Angriffe im Netzwerk ausbreiten können.

Endpoint Security entwickelt sich zur strategischen Aufgabe
Lange Zeit wurde Endpoint Security primär als technisches Zusatzthema betrachtet. Heute gehört sie zunehmend zur zentralen Sicherheitsstrategie moderner Unternehmen.

Der Grund dafür liegt in der zunehmenden Komplexität digitaler Arbeitsumgebungen. Unternehmen arbeiten mit Cloud-Plattformen, mobilen Geräten, externen Partnern und hybriden Infrastrukturen. Dadurch entstehen dynamische IT-Landschaften, die sich laufend verändern.

Klassische Sicherheitsmodelle mit festen Netzwerkgrenzen reichen dafür oft nicht mehr aus. Moderne Sicherheitskonzepte orientieren sich deshalb stärker am sogenannten Zero-Trust-Prinzip: Kein Gerät und keine Verbindung wird automatisch als vertrauenswürdig eingestuft.

Endpoint Security übernimmt in diesem Modell eine zentrale Rolle. Geräte werden kontinuierlich überwacht, verdächtige Aktivitäten analysiert und potenzielle Bedrohungen automatisiert isoliert.
Dabei geht es längst nicht mehr nur um klassische Virenerkennung. Moderne Systeme analysieren Verhaltensmuster, erkennen ungewöhnliche Prozesse und reagieren in Echtzeit auf verdächtige Aktivitäten. Erfahren Sie mehr darüber: https://www.netwyl-informatik.ch/leistungen/endpoint-security/ .

Der Faktor Mensch bleibt entscheidend
Trotz technischer Fortschritte bleibt der Mensch einer der wichtigsten Sicherheitsfaktoren. Mitarbeitende arbeiten unter Zeitdruck, wechseln zwischen verschiedenen Anwendungen und treffen täglich zahlreiche Entscheidungen im digitalen Arbeitsalltag.

Gerade deshalb müssen Sicherheitslösungen heute möglichst unauffällig funktionieren. Systeme, die den Arbeitsfluss stören oder komplizierte Prozesse erzeugen, werden häufig umgangen oder ignoriert.

Viele Unternehmen kennen die Problematik: Sicherheitswarnungen werden reflexartig bestätigt, Updates verschoben oder Schutzmechanismen deaktiviert, um kurzfristig weiterarbeiten zu können.
Professionelle Endpoint Security versucht deshalb, Sicherheit möglichst automatisiert im Hintergrund bereitzustellen. Verdächtige Prozesse werden erkannt, bevor Nutzer aktiv eingreifen müssen. Sicherheitsrichtlinien werden zentral verwaltet und Updates automatisiert ausgerollt.
Dadurch sinkt nicht nur das Risiko technischer Fehler, sondern auch die Belastung interner IT-Abteilungen.

Transparenz wird zum entscheidenden Faktor
Ein zentrales Problem vieler Unternehmen besteht darin, dass sie ihre eigene Geräteinfrastruktur nur eingeschränkt überblicken. Gerade in wachsenden Organisationen entstehen schnell unkontrollierte Strukturen: ältere Geräte, vergessene Benutzerkonten oder Softwareinstallationen ausserhalb definierter Prozesse.

Ohne zentrale Transparenz wird Sicherheitsmanagement jedoch schwierig. Unternehmen müssen nachvollziehen können:
- Welche Geräte sind aktiv?
- Welche Systeme besitzen kritische Schwachstellen?
- Wo fehlen Updates?
- Welche Geräte greifen auf sensible Daten zu?
- Welche Sicherheitsvorfälle wurden erkannt?

Endpoint-Security-Lösungen liefern genau diese Sichtbarkeit. Sicherheitsverantwortliche erhalten einen zentralen Überblick über den Zustand aller Endgeräte und können Risiken frühzeitig erkennen.

Dadurch verändert sich auch die Rolle der IT-Abteilung. Statt ausschliesslich auf Vorfälle zu reagieren, können Risiken präventiv bewertet und priorisiert werden.

Warum Prävention wirtschaftlich relevanter wird
Die Kosten eines Cybervorfalls werden häufig unterschätzt. Neben direkten Schäden entstehen oft erhebliche Folgekosten durch Wiederherstellungsmassnahmen, externe Spezialisten, Produktionsunterbrüche oder rechtliche

Abklärungen.

Gerade kleine und mittlere Unternehmen verfügen häufig nicht über ausreichende Ressourcen, um längere Ausfälle problemlos aufzufangen. Ein einzelner Sicherheitsvorfall kann deshalb erhebliche Auswirkungen auf den laufenden Betrieb haben.

Deshalb gewinnt präventive Endpoint Security zunehmend an wirtschaftlicher Bedeutung. Unternehmen investieren nicht nur in Schutztechnologien, sondern auch in Prozesse, Monitoring und automatisierte Reaktionsmechanismen.

Dabei steht weniger maximale Komplexität im Fokus als vielmehr Zuverlässigkeit und Alltagstauglichkeit. Sicherheitslösungen müssen stabil funktionieren, ohne die Produktivität unnötig einzuschränken.

Schweizer Unternehmen stehen vor besonderen Anforderungen
In der Schweiz spielt neben technischer Sicherheit auch der Schutz sensibler Geschäfts- und Kundendaten eine zentrale Rolle. Datenschutz, regulatorische Anforderungen und steigende Erwartungen an digitale Sicherheit erhöhen den Handlungsdruck zusätzlich.

Gleichzeitig kämpfen viele Unternehmen mit einem strukturellen Fachkräftemangel im IT-Bereich. Interne Teams sind oft stark ausgelastet und können Sicherheitsaufgaben nur begrenzt zusätzlich übernehmen.

Deshalb gewinnen externe Sicherheitsdienstleistungen und Managed-Security-Konzepte zunehmend an Bedeutung. Unternehmen suchen nach Lösungen, die technische Sicherheit mit operativer Entlastung kombinieren.

Die Schweizer NetWyl Informatik GmbH begleitet Unternehmen im Bereich moderner Endpoint-Sicherheitslösungen und fokussiert sich dabei insbesondere auf KMU und hybride Arbeitsumgebungen. Ziel ist es, Sicherheitsrisiken frühzeitig sichtbar zu machen und Endgeräte zentral abzusichern, ohne die tägliche Arbeit unnötig zu erschweren.

Im Mittelpunkt stehen dabei Lösungen, die Transparenz, Schutz und zentrale Verwaltung miteinander verbinden - insbesondere in Umgebungen mit mobilen Arbeitsplätzen und Cloud-Anwendungen.

Cyberangriffe werden professioneller
Cyberkriminalität hat sich in den vergangenen Jahren stark professionalisiert. Angriffe erfolgen automatisiert, arbeitsteilig und zunehmend datengetrieben. Schadsoftware wird laufend angepasst, um klassische Schutzmechanismen zu umgehen.

Besonders problematisch ist dabei die Geschwindigkeit moderner Angriffe. Zwischen der Kompromittierung eines Geräts und der Ausbreitung innerhalb eines Netzwerks liegen oft nur wenige Minuten.

Endpoint Security gewinnt deshalb vor allem durch ihre Fähigkeit an Bedeutung, Bedrohungen frühzeitig zu erkennen und automatisiert zu reagieren. Systeme isolieren kompromittierte Geräte, stoppen verdächtige Prozesse oder verhindern unautorisierte Zugriffe noch während eines laufenden Angriffs.

Dadurch reduziert sich das Risiko grossflächiger Schäden erheblich. Hier erfahren Sie mehr darüber: https://www.netwyl-informatik.ch/ .

NetWyl Informatik GmbH

Täschmattstrasse 19
6015 Luzern

PiotrKusak von Wyl

+41 41 520 07 40

piotr.kusak@netwyl-informatik.ch

www.netwyl-informatik.ch

Portrait

Die NetWyl Informatik GmbH mit Sitz in Luzern ist ein spezialisierter Schweizer IT-Dienstleister für Cybersecurity und Netzwerklösungen. Das Unternehmen unterstützt KMU sowie größere Organisationen bei der Absicherung ihrer IT-Infrastrukturen durch maßgeschneiderte Sicherheitskonzepte, Managed Security Services, E-Mail-Security, Cloud-Lösungen und Sicherheitsanalysen. NetWyl kombiniert langjährige IT-Security-Expertise mit persönlicher Beratung und verfolgt das Ziel, Unternehmen zuverlässig vor Cyberrisiken zu schützen und einen sicheren, stabilen IT-Betrieb zu gewährleisten.

News-ID: 1315781 • Views: 64 (Stand: 28.06.2026)

Link zur Pressemitteilung:

https://www.openpr.de/news/1315781/Endpoint-Security-Wenn-Endgeraete-zum-Risiko-werden.html