Lookout®

WHITEPAPER

Gibt es Vertrauen in **Zero Trust** Modellen? Mit Post Perimeter Security in einer neuen mobilen Arbeitswelt.

Drei wichtige Fakten müssen Unternehmen beim Schutz ihrer Ressourcen vor Datenverlust und Angriffen berücksichtigen:

1. Die Netzwerkgrenzen verschwimmen.
2. Konventionelle Sicherheitstechnologien greifen nicht.
3. Geräte sind nicht automatisch vertrauenswürdig.

Da immer mehr Mitarbeiter eine Mischung aus verwalteten und unverwalteten Geräten verwenden, ist eine neue Sicherheitsarchitektur erforderlich: **Post Perimeter Security**

DAS PROBLEM: Die Netzwerkgrenzen verschwimmen.

Die Arbeitsweise vieler Menschen hat sich mittlerweile grundlegend verändert. Kritische Daten werden in die Cloud verlagert und Mitarbeiter können über jedes beliebige Netzwerk darauf zugreifen, egal, wo sie sich gerade befinden. Und so müssen sie sich oft nicht einmal über ein VPN anmelden, um unterwegs ihre geschäftlichen E-Mails abzurufen oder vertrauliche Dokumente zu öffnen bzw. herunterzuladen.

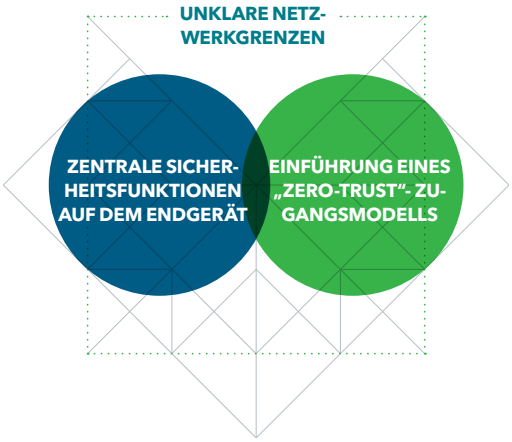
> **„Gartner schätzt, dass 80 % aller Arbeitsaufgaben bis 2020 über Mobilgeräte erledigt werden."**
>
> – Gartner, „Prepare for Unified Endpoint Management to Displace MDM and CMT", Juni 2018

Der aufgeweichte Perimeterschutz lädt außerdem zu Phishing-Attacken und anderen Angriffsformen ein. Hinzu kommt, dass Unternehmensgeräte mittlerweile auch privat genutzt werden. Social-Media-Apps, Messenger usw. schaffen eine Umgebung, die es Angreifern leicht macht, Mitarbeiter mit Phishing in die Falle zu locken und geschäftliche Zugangsdaten über persönliche Interaktionen auszuspähen. Bisher wurde in diesem Jahr bei 50,8 % der Lookout-Nutzer, die die Funktion zum sicheren Surfen aktiviert hatten, ein Phishing-Link erkannt.

50,8 % der Lookout-Nutzer, die das sichere Surfen aktiviert hatten, haben in diesem Jahr bisher einen Phishing-Link erkannt.

Mobilität und der nahtlose Datenzugriff sind starke Produktivitätsmotoren für Unternehmen, stellen jedoch auch eine große Herausforderung für Sicherheitsteams dar, die den Netzwerkrand bisher mit Firewalls und sicheren Web-Gateways schützen.

Tatsächlich aber befinden sich Unternehmensdaten längst nicht mehr nur innerhalb der Netzwerkgrenzen. Vielmehr bewegen sie sich fließend über diese Grenzen hinweg und sind damit besser zugänglich. Angesichts dieses Wandels kommen zwei neue Sicherheitsanforderungen auf:



Verlagerung zentraler Sicherheitsfunktionen auf das Endgerät

Zunächst einmal gilt es, die eigentlichen Sicherheitsmechanismen auf das Endgerät zu verlagern, anstatt die Endgeräte hinter den konventionellen Perimeterschutz zu bringen. Schließlich wäre es ja auch nicht sinnvoll, Wachen vor einer Burg zu postieren, wenn die Burg selbst keine Mauern mehr hat. Sie müssen sich überall dort absichern, wo sich Ihre Daten befinden.

Einführung eines „Zero-Trust"-Zugangsmodells

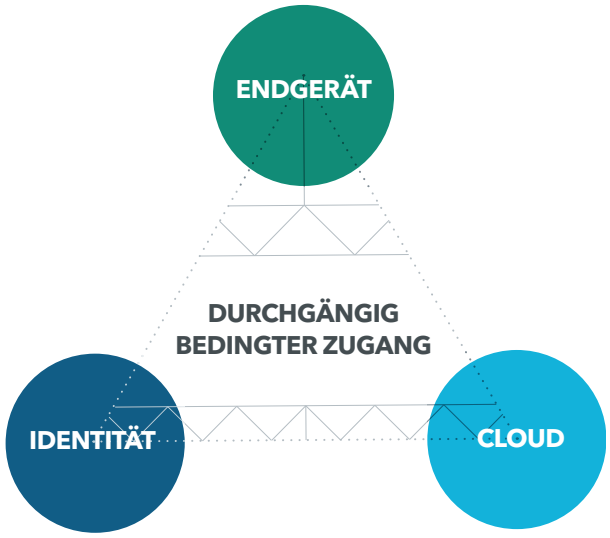
Selbst wenn sich die Sicherheitsmechanismen auf dem Endgerät befinden, darf ein Unternehmen das Gerät nie automatisch aus vertrauenswürdig einstufen, sondern erst prüfen. In dieser neuen Welt ist es unerlässlich, den Systemzustand aller Geräte routinemäßig zu prüfen, bevor ihnen Zugang zu Unternehmensdaten gewährt wird.

> „Zero Trust (kein Vertrauen): Dieser Begriff stammt aus einem Forschungsbericht von 2013, den Forrester im Auftrag des NIST erstellt hatte (Titel: Developing a Framework to Improve Critical Infrastructure Cybersecurity). Die Studie basierte auf früheren Arbeiten (ab 2004) des Jerricho Forum zur Aufweichung des Netzwerkrands."

DIE NEUE SICHERHEITSARCHITEKTUR: Sicherheit über die Netzwerkgrenzen hinaus

In der Praxis bedeutet das, dass eine neue Sicherheitsarchitektur her muss; ein Konzept, das wir als „Sicherheit über die Netzwerkgrenzen hinaus" bezeichnen. Es besteht im Grunde aus drei miteinander verbundenen Kernkomponenten:

- Endgeräteschutz
- Zugriff auf die Cloud
- Identitätsprüfung



Die Analyse des Geräterisikos mithilfe einer Endgeräteschutzlösung ist ein entscheidender Aspekt der Sicherheitsarchitektur in einer Welt verschwimmender Netzwerkgrenzen. Dieser Schutz liefert kontinuierlich Einblicke in Bedrohungen oder Risiken auf dem Gerät selbst. Die Lösung entscheidet dann, ob das Gerät eines Mitarbeiters sicher genug ist, um sich für den Zugriff auf Unternehmensressourcen anzumelden. Durch diesen Schutzmechanismus können Richtlinien auf Basis der spezifischen Risikotoleranz eines Unternehmens durchgesetzt werden – in Echtzeit.

Der derart eingeschränkte Zugriff auf die Unternehmens-Cloud und das Internet im Ganzen, ohne sich auf den üblichen Netzwerkschutz zu verlassen, ist ein weiterer Aspekt dieser Architektur. Hierfür müssen einige dieser zentralen Sicherheitsfunktionen auf das Endgerät verlagert werden, darunter die Überwachung auf manipulierte Links und Websites. Damit einhergehend muss auch verhindert werden, dass Mitarbeiter gefährliche Inhalte öffnen.

Diese beiden Aspekte gehen Hand in Hand mit einer Identitätslösung –z. B. von einem Anbieter für die Einmalanmeldung (Single-Sign-on, SSO) –, die Mitarbeitern entweder erlaubt, sich anzumelden und auf Unternehmensressourcen zuzugreifen, oder ihnen erst gar nicht die Möglichkeit zur Authentifizierung zu gibt. Nach erfolgter Anmeldung wird das Risiko des Endgeräts kontinuierlich überprüft, und sobald ein neues Risiko erkannt wird, wird der Zugriff verwehrt. In bestimmten Szenarien kann anstelle der Identitätsprüfung der Zugriff über ein Enterprise-Mobility-Management-Tool (EMM, z. B. bei verwalteten Geräten) oder ein Mobile-Application-Management-Tool (MAM) gesteuert werden.

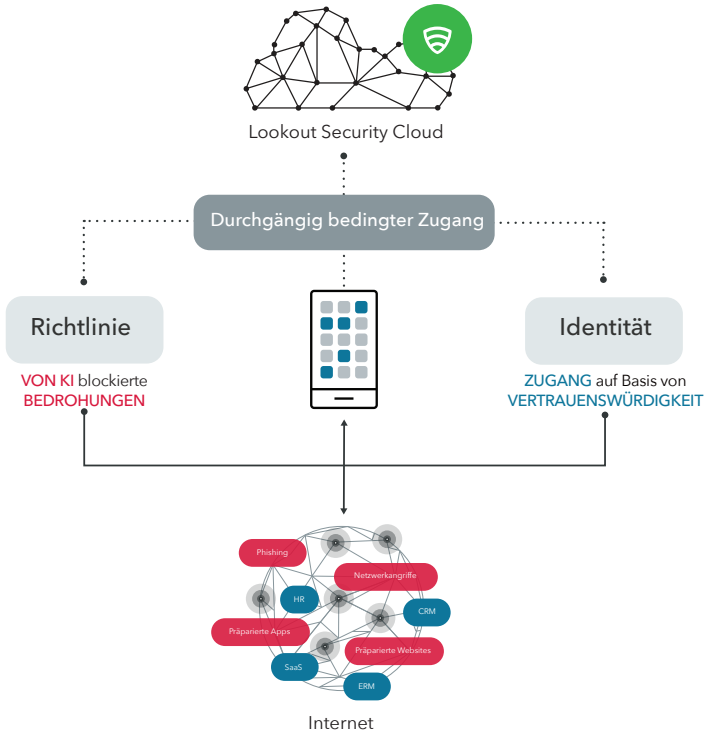
Durchgängig bedingter Zugang

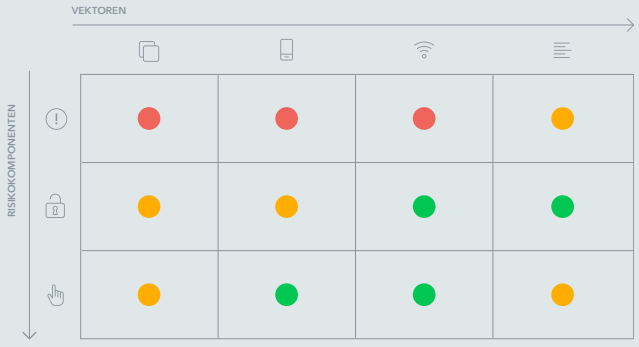
Wir bezeichnen die kontinuierliche Prüfung der Risiken und die entsprechende Steuerung des Zugriffs auf Ressourcen als „durchgängig bedingten Zugang". Konkret bedeutet das, dass die drei Kernfunktionen von „Post Perimeter Security" stets aktiv sind und sicherstellen, dass die Risikoschwellen Ihres Unternehmens nicht überschritten werden. Wenn doch, wird der Zugriff verweigert, um Ihre Unternehmensressourcen zu schützen.

DIE LÖSUNG: So bleiben Sie mit Lookout auch in Zeiten verschwimmender Netzwerkgrenzen sicher

Lookout hat seine Plattform speziell dafür entwickelt, dass Unternehmen die Geräte ihrer Mitarbeiter auch über die Netzwerkgrenzen hinaus schützen können.

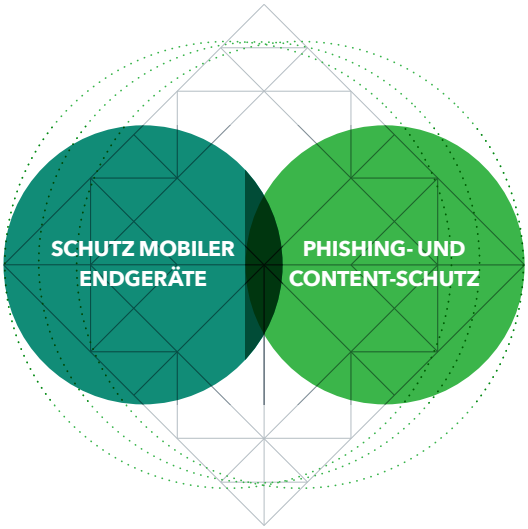
Grundlage dafür sind Sicherheitstelemetriedaten von mehr als 170 Millionen Geräten und 70 Millionen Apps weltweit. Diese Daten geben uns einen beispiellosen Einblick in das gesamte Risikospektrum, von geräte-, netzwerk- und appbezogenen Risiken bis hin zu Content-Bedrohungen. So können wir Unternehmen jederzeit sofort einen umfassenden Überblick über potenziell gefährliche Szenarien verschaffen, die sich auf einem Mitarbeitergerät abspielen.





Das Spektrum mobiler Risiken ist so groß, dass jedes Unternehmen irgendwann betroffen ist. Erfahren Sie mehr darüber und wie Sie mit der Matrix für mobile Risiken die Risikotoleranz Ihres Unternehmens einschätzen können.

WEITERE INFORMATIONEN



Durch den Schutz mobiler Endgeräte

Mit Lookout Mobile Endpoint Security können Unternehmen den geräteunabhängigen Zugriff auf Unternehmensdaten kontinuierlich prüfen und Zugangsberechtigungen vom vorhandenen Risiko abhängig machen. Damit ist zweierlei gewährleistet: Richtlinien werden jederzeit durchgesetzt und die Geräteintegrität wird geprüft, bevor sich Mitarbeiter an Unternehmensressourcen anmelden und auch während des Zugriffs.

Dabei haben Unternehmen die Möglichkeit, Richtlinien auf Basis ihrer Risikotoleranz auszuwählen, die dafür sorgen, dass die Geräte interne und externe Anforderungen erfüllen. Überschreitet ein Gerät das vom Unternehmen als akzeptabel definierte Risiko, so sendet Lookout eine Meldung an den Mitarbeiter, damit dieser das Risiko beseitigt. Auch der Administrator wird über die Mobile Endpoint Security-Konsole von Lookout informiert und der Mitarbeiter wird von sämtlichen Unternehmensressourcen abgemeldet.

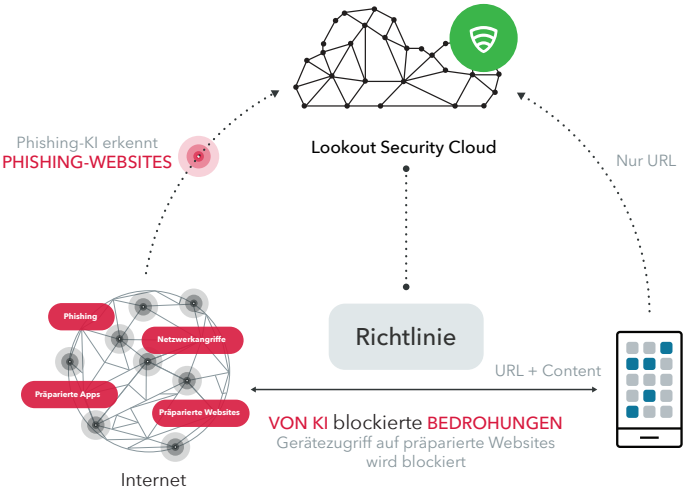
Erst, wenn das Gerät wieder eine akzeptable Risikostufe erreicht – in der Regel durch Abhilfemaßnahmen des Mitarbeiters – ist es dem Mitarbeiter gestattet, sich an den Unternehmensressourcen anzumelden.

Solange das Gerät unbeeinträchtigt ist, können die Mitarbeiter frei auf die Ressourcen zugreifen.

Durch Phishing- und Content-Schutz

Früher versuchten Unternehmen, Phishing-Risiken mit E-Mail-Sicherheitsfunktionen und Gateways am Netzwerkrand Herr zu werden. Zwar sind solche E-Mail-Sicherheitsfunktionen in der heutigen Sicherheitslandschaft noch immer notwendig und berechtigt, dennoch gibt es dabei ein Problem. Wenn Mitarbeiter über Geräte, die sich nicht innerhalb der Netzwerkgrenzen befinden, mit E-Mail- und anderen Anwendungen auf Daten zugreifen, dann genügen die herkömmlichen Sicherheitstechnologien nicht mehr.

Dies ist einer der Hauptgründe, warum Sicherheitsfunktionen auf das Endgerät verlagert werden müssen. Der Phishing- und Content-Schutz von Lookout residiert auf dem Endgerät und überwacht es auf Phishing-Attacken aus vielen Bedrohungsvektoren wie Social-Media-Apps, Messengern, SMS und jeder App, die eine Netzwerkverbindung herstellt.



Die Erkennungs-Engine von Lookout basiert auf künstlicher Intelligenz und ermittelt proaktiv den Ruf von Websites im Internet. Da Lookout dabei fortlaufend aktiv ist, erkennt die KI Phishing-Pakete bereits, während sie erstellt werden, also noch bevor der erste Angriff erfolgt. Unseren Erkenntnissen können Sie hier folgen: @PhishingAI.

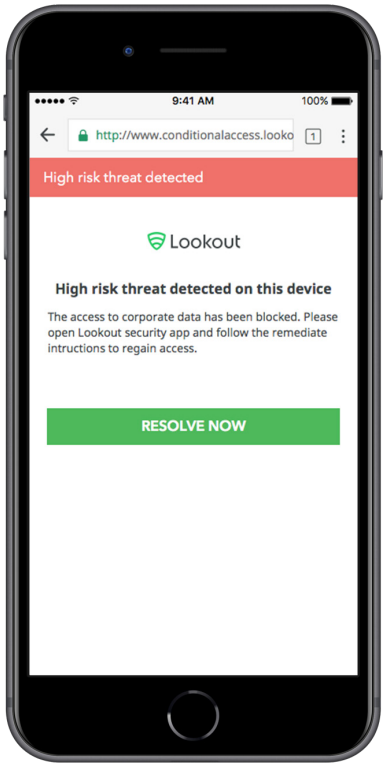
„Die Absicherung mobiler Endgeräte ist für uns von oberster Priorität. Wir betrachten Lookout als wesentlich, um unsere Unternehmensdaten vor Angriffen zu schützen und sämtliche Datenschutzvorschriften einzuhalten."

Christian Jösch, Netzwerkadministrator, Simon Hegele

Phishing auf Mobilgeräten 2018: Irrtümer und Fakten im Geschäftsalltag

BERICHT HERUNTERLADEN

DAS ERGEBNIS:
In dieser neuen Welt sind auch unverwaltete Geräte sicher



Unsere Arbeitsweise hat sich verändert. Laut IDC (International Data Corporation) wird erwartet, dass der Anteil der Mitarbeiter, die von großen US-Unternehmen als „mobil" eingestuft werden, in den nächsten 12 bis 18 Monaten von 35 % auf 43 % steigen wird.[1]

Die Art und Weise, wie Daten heute gespeichert werden, das Maß an Mobilität der Mitarbeiter sowie die unzähligen Geräte, die auf Unternehmensressourcen zugreifen, befeuern die rasante digitale Transformation, der Unternehmen sich nicht verschließen dürfen, wenn sie nicht den Anschluss verlieren wollen. „Mobiles Endgerät" entwickelt sich zunehmend zur Universalbezeichnung für sämtliche Geräte, mit denen Mitarbeiter ihre Arbeit erledigen.

Die klassischen Netzwerkgrenzen, wie wir sie bisher kannten, verschwimmen. Herkömmliche Sicherheitstechnologien greifen nicht mehr. Die verwendeten Geräte dürfen nicht automatisch als vertrauenswürdig eingestuft werden, doch es gibt Mittel und Wege, die Unternehmensressourcen auch in Zeiten schwindender Grenzen zu schützen. Sicherheit über die Netzwerkgrenzen hinaus ist die notwendige und zentrale Architektur für eine neue Ära des Arbeitens.

[1] Quelle: IDC, „The State of Mobile Enterprise Devices in 2018: An IDC Survey of Devices, Decisions, and Deployments", Veröffentlichung voraussichtlich im Oktober 2018