INFO SHEET

CLOUD- & VDI-WORKSPACES. ENDLICH SICHER MIT IGEL.

Edge Security fordert Unternehmen heraus. IGEL hat die Lösung.

IGEL OS, das Next-Gen Edge-Betriebssystem für Cloud Workspaces, überzeugt weltweit mit einem revolutionär einfachen, cleveren und sicheren Lösungsansatz für End User Computing und Cloud-basierte Arbeitsplätze. Der Bedarf ist riesig: Denn das Thema Sicherheit muss aggressiv über alle Bereiche der IT-Architektur angegangen werden – von der innersten Hard- und Software im Rechenzentrum oder der Cloud bis hin zu den Endgeräten. Aber wie lässt sich die immer aufwendigere Endpoint-Security radikal verschlanken? Die Lösung ist simpel: Ersetzen Sie Windows und andere Betriebssysteme einfach durch IGEL OS!

Jeden Tag begegnen Unternehmen einer wachsenden Vielfalt an Sicherheitsrisiken. Die verwundbarsten Punkte der IT-Security befinden sich dabei am „Rand“ ihres Netzwerks. In diesem Edge-Bereich brauen sich unterschiedlichste Kräfte zu einem wahren Sturm an potenziellen Endpoint-Bedrohungen zusammen. Einige davon sind seit Jahrzehnten bekannt, andere sind eher neu. Einige Beispiele:

- **Work from Home/Home-Office Security**
- **Immer weiter entwickelte Malware/Ransomware**
- **Patching: Endgeräte-OS und Anwendungen**
- **Höhere Ansprüche auf der Nutzerseite**

WORK FROM HOME/HOME OFFICE SECURITY

Die Corona-Pandemie hält die Welt in Atem und stellt tägliche Routinen, Operationen und Verhaltensweisen in Frage. Kein Land, kein Unternehmen, kein Mensch bleibt davon verschont. Seit März 2020 mussten die meisten Unternehmen ihre Arbeitsplätze kurzfristig ins Home-Office verlegen. Zwar besteht der Trend zum „Work from Home“ (WFH) schon eine ganze Weile, doch erst die COVID-19-Pandemie machte ihn von einem Tag auf den anderen zur Grundlage für die Geschäftskontinuität.

Auch nach der anfänglichen „Notfallsituation“ lassen viele Organisationen den Großteil ihrer Belegschaft ganz oder teilweise weiter von zu Hause arbeiten. Schließlich bringt WFH viele Vorteile mit sich: Die Endbenutzer genießen mehr Freiheit, der Arbeitgeber spart Geld, der ökologische Fußabdruck schrumpft. Auf der anderen Seite strapaziert WHF aber in hohem Maße die Sicherheit. So ist etwa die Verwaltung und Kontrolle von Unternehmensrichtlinien und Berechtigungen für eine weit verstreute Nutzerschar schwierig. Insbesondere, wenn diese verschiedenste Endgeräte nutzt: private, vom Unternehmen zur Verfügung gestellte oder beides. Erschwerend kommt hinzu, dass die meisten Endgeräte off-network, d.h. nicht mehr im Firmen-LAN konfiguriert, sind.

Unter diesen Umständen gewinnen IT-Teams kaum noch genügend Einblick und können nur schwer für alle Endpunkte das bisherige Maß an Wartung und Support gewährleisten, ohne für jeden einzelnen Fall eine teure VPN-Verbindung aufzubauen. Verstärktes WFH bereitet deshalb große Kopfschmerzen – nicht nur angesichts der limitierten Möglichkeiten für Verwaltung, Kontrolle, Troubleshooting und Support, sondern auch aus Kostengründen.

IMMER WEITER ENTWICKELTE MALWARE/RANSOMWARE

Seit Jahrzehnten stellt Malware die Unternehmens-IT vor immer neue Herausforderungen Dabei kämpfen kriminelle Hacker und Entwickler von Anti-Malware-Software unablässig um den entscheidenden Vorsprung. Fortschritte seitens der Anti-Malware, die zusätzlich zur Signatur-Erkennung auch das Verhalten von Schadprogrammen analysiert und mit bekannten Mustern vergleicht, beantworten Cyberkriminelle mit immer raffinierteren Methoden. In die Kategorie „besonders perfide und wiederkehrend“ fällt erpresserische Ransomware. Einmal in die IT-Infrastruktur oder den Speicher einer Organisation eingedrungen, kompromittiert sie Daten, um für ihre Freigabe ein Lösegeld zu erpressen. Nicht selten gehen Forderungen in die Millionen. Weil Schadsoftware typischerweise die Endpoints ins Visier nimmt, begegnen Organisationen mit einigen hundert bis vielen tausend Benutzern täglich der Gefahr einer „Headline Grabbing“-Attacke, die unbedarfte Mitarbeiter mit verfänglichen Überschriften oder Betreff-Zeilen in die Falle lockt.

PATCHING: ENDGERÄTE-OS UND ANWENDUNGEN

Wer Windows auf einem Endgerät nutzt, kennt die lästigen Arbeitsunterbrechungen durch Updates und Patches. Natürlich muss jede Software irgendwann auf den neuesten Stand gebracht werden. Doch das Aktualisieren und Patchen von Betriebssystemen auf einem Endgerät, insbesondere unter Windows 10, belastet die Nutzer ebenso wie das IT-Team. Denn die Maßnahmen müssen geplant und rechtzeitig, wiederholt durchgeführt werden. Umgekehrt gefährden ausgelassene Aktualisierungen die Security, weil sicherheitsrelevante Korrekturen ausbleiben.

Zeitaufwendige Endpoint-Updates und Patches sind aber auch kostspielig. Dies wird besonders deutlich, wenn wiederkehrende Updates und Patches einen oder mehrere Neustarts erfordern. Im günstigsten Fall nutzen betroffene User die Zeit für eine Kaffeepause oder eine spontane Besorgung. Wenn sie Pech haben, ist der Prozess jedoch nach ihrer Rückkehr fehlgeschlagen, das Gerät ist anfälliger als zuvor und das lästige Spiel beginnt von vorn.

Allerdings ist es nicht damit getan, dass IT-Organisationen alle Patches planen und traditionell am „Patch-Dienstag“ durchführen. Vielmehr müssen sie auch sicherstellen, dass auf jedem einzelnen Gerät die richtige Software aktualisiert wird, und das alles richtlinien- und rechtekonform. Mit steigender Installationsbasis wird diese Aufgabe nicht nur immer zeitraubender und fehleranfälliger, sondern eröffnet zahlreiche Sicherheitsrisiken.

HÖHERE ANSPRÜCHE AUF DER NUTZERSEITE

WFH und Enduser Mobility haben die Art und Weise verändert, wie unsere Mitarbeiterinnen und Mitarbeiter arbeiten. Was sich jedoch nicht geändert hat, ist die Erwartungshaltung seitens der Anwender, die mehr denn je ein überzeugendes und realitätsgetreues Nutzererlebnisse einfordern. Tatsächlich sind die Ansprüche gestiegen, seit die Menschen mehr Zeit am Computer verbringen und multimedial zusammenarbeiten. Ganz gleich, ob sie sich ein Schulungs-, Technik- oder Verkaufsvideo ansehen, an einer virtuellen Veranstaltung teilnehmen oder an einer Videokonferenz mit Teamkollegen über ein Unified Communications-Tool wie Microsoft Teams, Zoom, WebEx oder GoToMeeting: die Anwender erwarten Qualität. Ohne Tonaussetzer, Bildhänger und andere Störungen.

Die neue mobile Freiheit und die gestiegene Erwartungshaltung setzen IT-Teams zusätzlich unter Druck. Denn unter Umständen haben diese bereits andere Probleme: etwa die wachsende Zahl privat genutzter Endgeräte, die oft zu wenig Prozessorleistung oder Speicher bieten. Oder netzwerkfremde Hürden wie geringe Bandbreiten oder die berüchtigte „letzte Meile“ zum Wohnort, mit denen viele Nutzer zu kämpfen haben.

Es ist ein Dilemma: Auf der einen Seite soll die IT die Nutzer zufrieden stellen, auf der anderen die vollständige Sicherheit und Kontrolle über sämtliche Endgeräte erlangen. Wie lässt sich beides gleichzeitig erreichen, ohne das andere zu gefährden?

DIE ENDPOINT-LÖSUNG BEGINNT MIT DEM OS

Der erste Schritt zur Bewältigung der oben genannten Herausforderungen besteht darin, Windows ins sichere Rechenzentrum oder die Cloud zu verlagern. Gleichzeitig bekommen alle Endpoints ein einheitliches Betriebssystem, das speziell für den einfachen und sicheren Workspace-Zugriff konzipiert ist - IGEL OS.

IGEL OS basiert auf Linux und zeichnet sich durch geringen Platzbedarf, ein modulares, die Angriffsfläche minimierendes Design sowie durch einen Read-only-Zugriff aus, der Firmware-Manipulationen verhindert. Dank dieser Eigenschaften kann IGEL OS den Zeit- und Kostenaufwand für Edge-Security drastisch reduzieren.

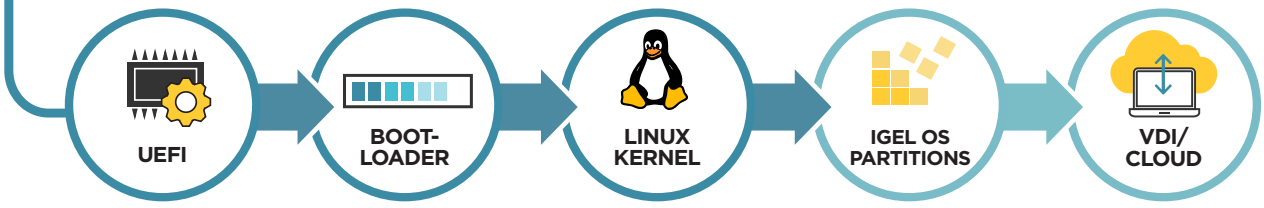
DIE IGEL-CHAIN-OF-TRUST

- Stellt sicher, dass alle Komponenten eines VDI/Cloud Workspace-Szenarios sicher und vertrauenswürdig sind.
- Beim Start einer Komponente wird automatisch die kryptographische Signatur der folgenden Komponente geprüft. Diese wird nur dann gestartet, wenn sie von einer vertrauenswürdigen Stelle signiert ist (z.B. IGEL, UEFI Forum).
- Wird bei einem beliebigen Schritt ein Fehlverhalten erkannt, wird der Endbenutzer gewarnt und die IT-Abteilung kann entsprechende Maßnahmen ergreifen

DAS VERFAHREN

1. Die softwarebezogene IGEL-Vertrauenskette beginnt mit UEFI.
2. UEFI prüft den Bootloader auf seine UEFI Secure Boot Signatur.
3. Der Bootloader prüft dann den IGEL OS Linux-Kernel.
4. Wenn die Signaturen der OS Partitionen korrekt sind, wird IGEL OS* gestartet und die Partitionen werden gemountet.
5. Für Anwender, die eine Verbindung zu einer VDI- oder Cloud Umgebung herstellen, überprüft eine Zugangssoftware das Zertifikat des angeschlossenen Servers.

** IGEL OS 11.03 und höher*



An IGEL-OS beißen sich Angreifer die Zähne aus. Dass es äußerst schwer zu attackieren ist liegt nicht zuletzt an der sogenannten „Chain of Trust“, einer schwer zu überwindenden Abfolge kryptografischer Signaturprüfungen. Diese „Vertrauenskette“ beginnt auf dem System-on-Chip (SoC) bestimmter IGEL-Endpoints, bei allen anderen Geräten im Unified Extensible Firmware Interface (UEFI), und setzt sich bis zum VDI oder Cloud Workspace fort.

Wird ein Endpoint mit IGEL-OS neugestartet, stellt die Chain of Trust sicher, dass während der Startsequenz keine Schlüsselprozesse in Firmware und Software verändert wurden. Taucht in irgendeinem Glied der Kette ein Fehler auf, alarmiert der Mechanismus den Endanwender, und die IT-Abteilung kann entsprechende Maßnahmen ergreifen.

IGEL OS läuft auf jedem x86-64-kompatiblen Gerät mit 1 GHz-Prozessor und 2 GB RAM oder höher. Außerdem eignet sich das plattformunabhängige Betriebssystem hervorragend zur Vereinheitlichung typischer Endgeräte wie PCs und Laptops sowie Thin Clients von Dell, HP, Lenovo und anderen. IGEL-Geräte miteingeschlossen entsteht so eine einheitliche OS-Plattform für sämtliche betrieblich genutzten Endpoints.

Eine weitere, hochinteressante Zugriffsmöglichkeit auf IGEL OS bietet der UD Pocket. Dieser USB-Endpoint von IGEL ist so klein wie eine Büroklammer und lässt sich an jedes kompatible Gerät anschließen. Firmenfremde PCs oder Laptops werden so nach dem Booten per USB sofort zum IGEL OS Endpoint für den gewohnten Zugriff auf den persönlichen Workspace oder bestimmte Cloud Anwendungen. Um einzig diesem Zweck zu dienen, läuft das IGEL OS in einem vollständig sicheren, separaten Container. Alle Daten verbleiben in der sicheren Cloud. Mit diesen Eigenschaften wird der UD Pocket in zweierlei Hinsicht zur idealen Lösung: Zum einen lässt er den Anwendern zu Hause und an anderen Orten außerhalb des Firmennetzwerks größtmögliche Freiheiten, einschließlich der Wahl ihres Endgeräts. Zum anderen profitiert das Unternehmen von einer umfänglichen Verwaltung und vollständigen Kontrolle über jeden einzelnen IGEL Endpoint. Wird der UD Pocket getrennt, kehrt das private Gerät wieder zum Standard-OS und seiner Standardkonfiguration zurück.

SECURE BY DESIGN: ENDPOINT-MANAGEMENT UND -KONTROLLE

Die minimale Angriffsfläche und inhärente Sicherheit einschließlich Chain of Trust qualifizieren IGEL OS als vertrauenswürdiges Betriebssystem für eine weit verteilte Nutzerbasis im Home-Office. Aber es kommt noch besser: Denn in Kombination mit der IGEL Universal Management Suite (UMS) lassen sich IGEL OS Endpoints hocheffizient verwalten und kontrollieren. Dazu können Endbenutzerrichtlinien und -berechtigungen wahlweise aus dem Active Directory übernommen, oder einfach über die UMS-Konsole erstellt werden. Egal, welcher Weg gewählt wird, und ob es sich um einige hundert oder zehntausend Endgeräte handelt: Über die UMS-Konsole stellen IT-Teams problemlos sicher, dass jeder IGEL OS Endpoint für den jeweiligen Anwender mit dem korrekten IGEL OS Image konfiguriert ist.

Darüber hinaus sorgt der modulare Aufbau der IGEL OS dafür, dass einige Anwender mit „noch weniger“ IGEL OS auf ihrem Endgerät arbeiten als andere. Weil der OS-Footprint für jedes einzelne Gerät so klein wie möglich ausfällt, minimiert sich auch die Angriffsfläche. Sicherheitstechnisch hochrelevant ist auch, dass die UMS sämtliche Endgeräte mit IGEL OS stets mit der neuesten Version des IGEL-Betriebssystems versorgt. Im Vergleich zu Windows 10 sind diese Firmware-Updates

und Patches jedoch deutlich kleiner und viel seltener nötig. Ihre Verteilung erfolgt schnell und bandbreitenschonend über die „Buddy Update“-Technik. Sämtliche IGEL OS-Updates nutzen einen sicheren Tunnel zwischen der UMS und den zu aktualisierenden Endpoints.

Mit dem schlagkräftigen Doppel aus IGEL OS und UMS befreien sich IT-Teams von der Langeweile, dem Planungsirrsinn und der hohen Kostenbelastung der klassischen Endgeräte-Aktualisierung. Der Vorteil für die Anwender: Dass ein IGEL OS-Update stattgefunden hat, fällt fast gar nicht auf.

Und was ist mit „off-network“? IT-Verantwortliche, die Geräte außerhalb des Firmen-LANs genauso effizient verwalten und kontrollieren wie auf dem Firmencampus, können dies mithilfe des IGEL Cloud Gateway (ICG) erreichen. Das ICG baut zum Gerät des Remote-Nutzers eine sichere, verschlüsselte Verbindung auf – ganz ohne VPN-Service und VPN-Verbindung. Darüber hinaus vereinfacht das ICG auch den Support. Mittels Shadowing können Helpdesk-Mitarbeiter den Nutzer-Bildschirm spiegeln, um akute Probleme zu lösen.

HAKEN SIE DAS THEMA ENDPOINT-SECURITY AB! FÜR IMMER.

CSOs, CIOs und IT-Leiter haben es heute mit einem Sturm an globalen Bedrohungen zu tun. Home-Office, Malware und Ransomware, Software-Updates und Patches, aber auch die steigende Performanceerwartung der Endbenutzer generieren jeweils für sich ganz spezifische Herausforderungen. Während Cyber-Kriminelle ihre Angriffe gezielt auf den Edge-Bereich richten, den verwundbarsten Punkt am Rand des Netzwerks.

Die wirksame Soforthilfe von IGEL – mögen es einige hundert, tausend oder zehntausend Endgeräte sein – lässt sich auf drei Begriffe reduzieren: IGEL OS – zum Download oder per UD Pocket –, IGEL UMS und IGEL Cloud Gateway.

Noch nicht überzeugt? Stellen Sie sich vor, wie es wäre, wenn Sie das Thema Sicherheit und Verwundbarkeit sämtlicher Endgeräte im Unternehmen praktisch abhaken könnten. Unabhängig davon, wie viele es sind , und wo sie sich befinden. Stellen Sie sich vor, Sie könnten die kostspieligen, mühsamen und zeitaufwändigen Windows-Updates und -Patches einfach eliminieren. Was glauben Sie, wie viel effektiver Ihre Malware-Abwehr wird, wenn Sie sich auf einen Ort konzentrieren können? Auf Rechenzentrum oder Cloud, statt auf einige hundert oder tausend Lokationen? Und zuletzt: Stellen Sie sich vor, dass all Ihre Nutzer, einschließlich Home-Office, produktiver, zufriedener und mit begeisternder User Experience arbeiten können. Und das alles auf dem Gerät ihrer Wahl, ohne dass sie – und Sie – unter einem „Overkill“ an Anwendungen und Antiviren-Software leiden. Dies alles ist möglich. Mit dem Edge-Betriebssystem der nächsten Generation für Cloud-Workspaces: IGEL OS.

BESUCHEN SIE UNS ONLINE: IGEL.DE/SECURITY-AT-THE-EDGE

IGEL. IT WORKS. SO YOU CAN.