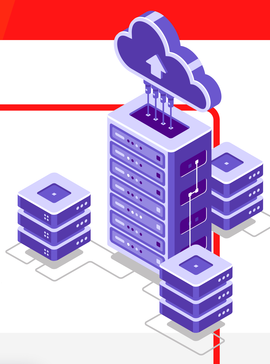
ivanti

IHRE REISE ZUR CYBERSICHERHEIT

Mit der raschen Verlagerung zur Remote-Arbeit sind viele Sicherheitslücken im neuen **„Everywhere Workplace“** aufgetaucht, sodass eine umfassende und skalierbare Cybersicherheitsstrategie erforderlich ist, um potenzielle Bedrohungen zu minimieren.

Hier sind sechs Schlüsselbereiche, die Sie auf dem Weg zu einer soliden Cybersicherheitsstrategie berücksichtigen sollten.

1. Vollständige Transparenz der Assets



Warum?

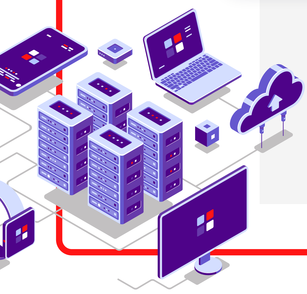
Man kann nicht verwalten, was man nicht kennt.

Ohne eine genaue Bestandsaufnahme der Assets (Cloud, Software, Hardware) ist Ihr Unternehmen anfällig für Sicherheitsrisiken.

Wie?

Verschaffen Sie sich einen vollständigen Echtzeit-Überblick über alle angeschlossenen Geräte, um Ihre IT-Infrastruktur besser zu verwalten, zu organisieren und zu optimieren.

2. Moderne Geräteverwaltung



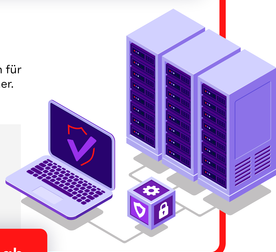
Warum?

Die Überwachung der Konformität von Remote-Benutzern und -Geräten ist für einen sicheren Betrieb von entscheidender Bedeutung, z. B. um Software auf dem neuesten Stand zu halten und Probleme schnell zu beheben.

Wie?

Setzen Sie UEM als Teil Ihrer Strategie ein.

3. Gerätehygiene etablieren



Warum?

Durch die Festlegung universeller Sicherheitsanforderungen für alle Geräte wird die Problemdiagnose schneller und einfacher.

Wie?

Nutzen Sie die Automatisierung, um proaktiv alle mit der Gerätehygiene verbundenen Sicherheitsprobleme zu erkennen und zu verwalten.

4. Sichern Sie Ihre Benutzer ab

Warum?

Bei Passwörtern fehlt der Kontext (Gerät, Anwendung, Netzwerk, Bedrohung), sodass es unmöglich ist, autorisierte von nicht autorisierten Benutzern zu unterscheiden.

Wie?

Zero-Sign-On: Da es keine Passwörter gibt, gibt es auch keine Anmeldedaten/Passwörter, die gestohlen werden könnten.

5. Den richtigen Zugang gewähren

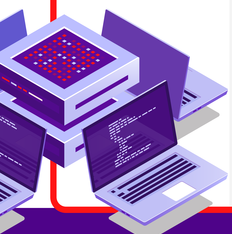
Warum?

Die Beschränkung der Benutzer auf die von ihnen benötigten Geschäftsressourcen minimiert zugangsbasierte Sicherheitsbedrohungen.

Wie?

Verwenden Sie einen vertrauenswürdigen Netzwerkzugang, um den Zugriff der Benutzer auf Unternehmensdaten zu verfolgen, zu überwachen und zu kontextualisieren.

6. Automatisierung von Compliance und Risikomanagement



Warum?

Die manuelle Verwaltung ist zeitaufwendig, ineffizient und birgt mehr Sicherheitsrisiken.

Wie?

Seien Sie proaktiv, nicht reaktiv: Setzen Sie eine universelle und automatisierte Strategie zur Einhaltung von Vorschriften und zum Risikomanagement ein.

Möchten Sie mehr über den Aufbau einer soliden Cybersicherheitsstrategie erfahren? Holen Sie sich “Managen, Automatisieren und Priorisieren Ihrer Reise zur Cybersicherheit” (Manage, Automate and Prioritize – MAP) jetzt:

E-Book herunterladen

ivanti