ivanti

Bericht zur Cyber-Sicherheit von Verbrauchern 2021:

Wie Remote-Arbeitskräfte Unternehmen dem Risiko eines Cyberangriffs aussetzen

Riskantes Verbraucherverhalten vergrößert die Lücke in der Cybersicherheit

Die Pandemie 2020 hat nicht nur ein tödliches und verheerendes Virus auf der ganzen Welt entfesselt, sondern auch jeden Aspekt unseres täglichen Lebens grundlegend verändert -einschließlich der Frage, wo und wie wir arbeiten. Mitarbeiter aller Art und in allen Branchen begannen, wann immer möglich, von zu Hause aus zu arbeiten. Obwohl Remote-Arbeitskräfte dazu beitrugen, kritische Geschäftsabläufe aufrechtzuerhalten, sehen sich viele Unternehmen nun mit einer dramatischen Zunahme von Cybersecurity-Bedrohungen konfrontiert, die auf den Zustrom ungesicherter persönlicher Geräte und riskantes Mitarbeiterverhalten zurückzuführen sind. Wie sieht die Bedrohungslandschaft mehr als ein Jahr nach Ausbruch der Pandemie jetzt aus?

Im Februar 2021 veröffentlichte Ivanti den „Bericht zur Cyber-Sicherheit von Verbrauchern 2021“, der die spezifischen Bedrohungen aufzeigt, die Unternehmen gefährden. Die Ergebnisse basieren auf einer landesweit repräsentativen Stichprobe von mehr als 2.000 Personen über 18 Jahren, die im November 2020 in den USA und Großbritannien arbeiteten.

Während sich Unternehmen der Schwachstellen bewusst sind, die durch nichtverwaltete, mitarbeitereigene Geräte und Apps entstehen, zeigt dieser Bericht, dass Mitarbeiter auch dann risikoreiches Verhalten an den Tag legen, wenn sie firmeneigene Computer für die Nutzung zu Hause erhalten. So gab beispielsweise einer von vier Verbrauchern zu, dass er seine Arbeits-E-Mail oder sein Passwort für den Zugriff auf Verbraucherwebsites und - Anwendungen wie Essenslieferungs-Apps, Online-Shopping-Seiten und sogar Dating-Apps verwendet.

Erschweren der Unternehmenssicherheit

Selbst wenn die Welt irgendwann zur „Normalität“ vor dem Corona-Virus zurückkehrt, wird das Ausmaß der Remote-Arbeit wahrscheinlich bleiben. Obwohl Unternehmen versucht haben, Sicherheitslücken bei ihren Remote-Mitarbeitern zu schließen, ist klar, dass sie mehr tun müssen, als nur unternehmenseigene Hardware und Software bereitzustellen. Ein genauerer Blick auf die Ergebnisse des Berichts sollte Unternehmen einen besseren Einblick in die bevorstehenden Herausforderungen geben.

ivanti

1 von 4 Verbrauchern

geben zu, dass sie ihre Arbeits-E-Mail oder ihr Passwort für den Zugriff auf Verbraucherwebsites und -anwendungen wie Essenslieferungs-Apps, Online-Einkaufsseiten und sogar Dating-Apps verwenden.

Sicherheitsgewohnheiten von Remote-Mitarbeitern gefährden ihr Unternehmen

Um das Sicherheitsniveau der durchschnittlichen Home-Office-Umgebung besser zu verstehen, wurden die Befragten zu ihrem Verhalten und ihren Sicherheitspraktiken für alle ihre Geräte, einschließlich der IoT-Geräte im Haus, befragt.

Recycelte Zugänge:
Fast ein Viertel der Befragten in den USA und fast jeder Fünfte in Großbritannien gaben an, dass sie ihre Arbeits-E-Mail oder ihr Passwort verwendet haben, um sich bei Verbraucherwebsites und Apps anzumelden.

Persönliche Geräte für den Arbeitszugang:
Fast die Hälfte aller Befragten in den USA und mehr als ein Drittel der Befragten in Großbritannien gaben an, dass sie ein persönliches Gerät wie einen Laptop, ein Smartphone, ein Tablet oder eine Smartwatch für den Zugriff auf Unternehmensanwendungen und -netzwerke verwenden dürfen.

Zwei-Faktor-Authentifizierung für IoT-Geräte:
Fast die Hälfte aller Befragten in den USA und Großbritannien hat keine Zwei FaktorAuthentifizierung für smarte Geräte in ihrem Zuhause eingerichtet.

Wichtigste Erkenntnis: Vernachlässigen Sie nicht die grundlegenden Sicherheitsmaßnahmen zu Hause

Das Fehlen grundlegender Sicherheitsvorkehrungen für heimische IoT-Geräte macht sowohl Remote-Mitarbeiter als auch ihre Unternehmen anfälliger für Cyberbedrohungen, wie zum Beispiel den Ring-Hack, der 2019 viral ging.

Schlechte Sicherheitsgewohnheiten, wie z. B. die Wiederverwendung von Passwörtern für den Zugriff auf Verbraucherwebsites, können für Unternehmen ein größeres Risiko für einen Verstoß darstellen. Organisationen müssen eine klare Trennung zwischen beruflich und privat genutzten Apps und Websites durchsetzen.

Unternehmenssicherheit ist auch bei Remote-Mitarbeitern unzureichend

Nach dem Ausbruch der Pandemie sahen wir einen dramatischen Anstieg von CybersecurityAngriffen gegen unsichere persönliche Geräte und IoT-Heimgeräte. Während schlechte Sicherheitsgewohnheiten der Endbenutzer teilweise Schuld daran sein können, ergab unsere Umfrage, dass Unternehmen die Sicherheit in wichtigen Bereichen verbessern können.

25%

Sicherheits-Software:
Mehr als 25 % aller Befragten gaben an, dass sie keine spezielle Sicherheitssoftware auf ihren Geräten installiert haben müssen, um auf bestimmte Anwendungen zuzugreifen, während sie remote arbeiten.

Passwort-Updates:
Rund 25 % der Remote-Mitarbeiter:innen in den USA und Großbritannien gaben an, dass ihr Unternehmen nicht verlangt, dass sie ihr Passwort alle sechs Monate aktualisieren oder einen Einmal-Passwortgenerator verwenden.

30%

Sichere Zugriffswerkzeuge:
Fast 30 % aller Befragten in den USA und Großbritannien gaben an, dass ihr Unternehmen von Remote-Mitarbeitern nicht verlangt, ein sicheres Zugangstool, wie z. B. eine VPN, zu verwenden.

Wichtigste Erkenntnis: Zero-Trust-Sicherheit ist unerlässlich

Der Remote-Arbeitsplatz ist auf dem Vormarsch. Obwohl die IT-Abteilung von Unternehmen die mobile Sicherheit in einigen Bereichen verbessert haben, müssen sie immer noch die sichere Authentifizierung auf allen Geräten verbessern, die Mitarbeiter für die Arbeit nutzen.

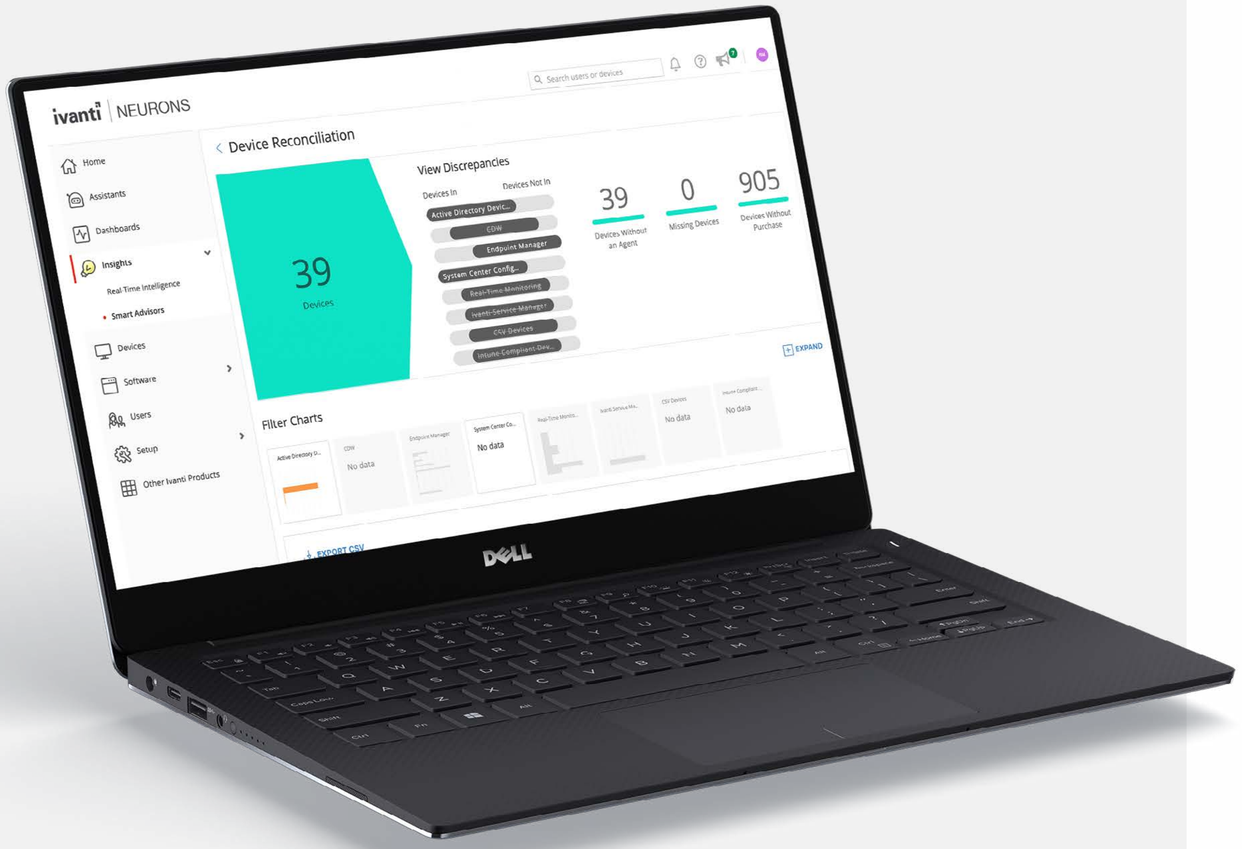
Durch die Implementierung einer Zero-Trust-Sicherheitsstrategie, die darauf abzielt, jeden Benutzer, jedes Gerät, jede App und jedes Netzwerk zu verifizieren, bevor der Zugriff auf Unternehmensressourcen gewährt wird, stellen CISOs sicher, dass die Mitarbeiter produktiv und sicher bleiben, egal wo sie arbeiten.

Sichere Verbraucher ermöglichen sichere Unternehmen

Da immer mehr Menschen remote arbeiten, hat sich die Bedrohungslandschaft schneller als je zuvor erweitert. Aus diesem Grund sollten Unternehmen die wichtigsten Strategien zum Schutz von Unternehmens-Apps und -Daten vor Lücken in der IoT-Sicherheit und dem Bewusstsein der Verbraucher zu Hause prüfen. Es ist klar, dass mit der zunehmenden Verbreitung von Consumer-Geräten Remote-Mitarbeiter Schwierigkeiten haben werden, erweiterte Sicherheitseinstellungen zu aktivieren und zu pflegen - und Cyberkriminelle wissen das. Infolgedessen hat die COVID-19-Pandemie nicht nur eine massive Bedrohung für die menschliche Gesundheit geschaffen, sondern auch unser Wohlergehen gefährdet, indem sie es Cyberkriminellen erleichtert hat, Menschen und Organisationen auszunutzen, die nicht ausreichend geschützt sind.

Es gibt jedoch eine gute Nachricht: Unternehmen können Zero Trust Security schon heute einführen

Unternehmen können bereits jetzt Schritte unternehmen, um Zero Trust-Protokolle für die gesamte Belegschaft zu implementieren. Mit einem Zero-Trust-Modell können Unternehmen das Risiko von gestohlenen Zugangsdaten eliminieren, indem sie sicherstellen, dass jeder, der auf Unternehmensdaten, Anwendungen oder Netzwerke zugreift, eine vertrauenswürdige Person ist. Darüber hinaus kann Zero Trust die Durchsetzung von Richtlinien zur akzeptablen Nutzung, einschließlich der Verwendung von Multifaktor-Authentifizierung, Geräteschutz und sicherer Netzwerkkonnektivität, erheblich erleichtern, da die Remote-Arbeit weiter zunimmt und sich die Geräte immer weiterverbreiten.



Metodologia

Die Ergebnisse des ersten Berichts zur Cyber-Sicherheit von Verbrauchern basieren auf einer Umfrage, die im November 2020 durchgeführt wurde. Die Studie sollte untersuchen, wie sich die Cyber-Sicherheitsgewohnheiten von Verbrauchern und Unternehmen im Laufe der Pandemie verändert haben. Für die Umfrage wurde eine landesweit repräsentative Stichprobe von 2.000 Einwohnern der USA und Großbritanniens über 18 Jahren verwendet, die von zu Hause aus an einem vom Unternehmen zur Verfügung gestellten Computer arbeiteten.

Über Ivanti

Die Ivanti-Automatisierungsplattform hilft, jede IT-Verbindung intelligenter und sicherer zu machen – über Geräte, Infrastruktur und Menschen hinweg. PCs und mobile Geräte, sowie virtuelle Desktop-Infrastrukturen und Rechenzentren erkennen, verwalten, sichern und warten Ivanti IT-Ressourcen von der Cloud bis zum Edge im „Everywhere Workplace“ – und bieten gleichzeitig personalisierte Mitarbeitererfahrungen. Am „Everywhere Workplace“ fließen Unternehmensdaten frei über Geräte und Server und ermöglichen es den Mitarbeitern, produktiv zu sein, egal wo und wie sie arbeiten. Ivanti hat seinen Hauptsitz in Salt Lake City, Utah, und verfügt über Niederlassungen auf der ganzen Welt. Für weitere Informationen besuchen Sie www.ivanti.com und folgen Sie @GoIvanti.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com