Dell Sicherheitspraktiken für Geräte

Drei Kriterien für die Schaffung von Gerätevertrauen

Dell CyberexpertInnen erläutern die entscheidende Rolle, die Gerätesicherheitspraktiken für die langfristige Ausfallsicherheit Ihres IT-Ökosystems spielen.

Autoren
Rick Martinez
Dell Fellow und Vice President

Eric Baize
VP, Product and Application Security

Einführung

Auf dem überfüllten Cybermarkt von heute werden Sie wahrscheinlich mit Optionen für Sicherheitsprodukte und -lösungen überflutet. Aber was wäre, wenn ich Ihnen sagen würde, dass der wichtigste Teil Ihrer Sicherheitsstrategie nicht Ihre Sicherheitsprodukte sind?

Als einer der führenden PC-Hersteller legt Dell großen Wert auf Sicherheit. In den letzten Jahren haben die verheerenden Folgen von Ransomware-Angriffen und die Verbreitung von firmwarebasierter Malware deutlich gezeigt, dass Endgeräte zunehmend zum Ziel von Angriffen werden. Leider können Einzelpunktlösungen – wie innovativ sie auch sein mögen – NutzerInnen und Daten nicht vollständig schützen.

Wenn Sie die Sicherheit Ihres bestehenden Ökosystems neu bewerten und nach Produkten für eine Aktualisierung suchen, sollten Sie neben der Kaufentscheidung auch berücksichtigen, wie Ihr PC-Hersteller mit dem Thema Sicherheit umgeht. Warum? Sie denken vielleicht, dass es um die Bewertung von Produkten geht, aber die Bewertung des Lieferanten ist ebenso wichtig. Ein vertrauenswürdiger und erfahrener Anbieter sicherer PCs, der die Bedrohungslage versteht, kann dieses Wissen nutzen, um Sie beim Schutz Ihres Unternehmens zu unterstützen, während sich dieses Umfeld weiterentwickelt. Mit diesem Partner können Sie ein Sicherheitsökosystem aufbauen, das unvermeidliche Angriffe intelligent abwehrt und langfristige Ausfallsicherheit bei Cyberangriffen fördert.

Sicherheit beginnt früher, als Sie denken

IT-EntscheidungsträgerInnen und EndnutzerInnen interagieren in der Regel mit einer Mischung aus VertriebsmitarbeiterInnen, Geräten und Produktsupport. Aber das ist nur die Spitze des Eisbergs, wenn es um Sicherheit geht. Warum? Es ist ähnlich wie bei der Lebensmittelsicherheit. Sie können die Lebensmittelsicherheit nicht allein anhand Ihrer Interaktion mit dem Servicepersonal in einem Restaurant beurteilen, denn Lebensmittelsicherheit beginnt in der Küche. Ebenso muss alles, was Geräte sicher macht, bereits vor der Herstellung eines Produkts vorhanden sein – und ist

daher selten sichtbar. Dell hat unzählige Entwicklungsstunden und intellektuelle Anstrengungen investiert, um die IT-Arbeitsumgebung seiner Kunden von Grund auf zu sichern – die komplexen Prozesse und Protokolle, die das Design, die Entwicklung und die Auslieferung jedes einzelnen Geräts regeln. Diese Arbeit, die niemand sieht, bildet die stabile Grundlage, auf der die sichersten Geräte entwickelt werden können. Diese Arbeit trägt dazu bei, die IT-Arbeitsumgebung der Kunden zu schützen, unabhängig davon, ob es sich um Kunden aus dem öffentlichen Sektor, Großunternehmen oder kleine und mittlere Unternehmen handelt. Dell ist davon überzeugt, dass moderne Sicherheit für alle Unternehmen, ob groß oder klein, möglich ist, und wir sind bestrebt, Lösungen zu liefern, die Ihr Unternehmen – und damit auch Ihre Kunden – schützen.

Unsere Verfahren für die Gerätesicherheit

Wenn wir über den Schutz unserer kommerziellen Geräte nachdenken, denken wir über Sicherheitsergebnisse nach, d. h. darüber, wie das Gerät zur allgemeinen Sicherheit eines Unternehmens beiträgt. Wie hilft das Gerät, Angriffe zu verhindern? Was sorgt für seine Sicherheit bei Angriffen? Und wie bleibt es während seiner gesamten Lebensdauer sicher?

Wie zu erwarten, verfügen wir über Dutzende von Praktiken zur Entwicklung sicherer kommerzieller PCs, die den Branchenstandards entsprechen und einen Zero-Trust-Sicherheitsansatz unterstützen. Heute möchte ich einige davon unter drei Kernthemen hervorheben: Sicherheit in der Lieferkette, Sicherheit im Code und Sicherheit bei der Nutzung.

1. Wir sichern unsere Gerätelieferkette. Das bedeutet strenge Kontrollen unserer Lieferketten für Hardware und Software, also für die physischen und digitalen Lieferketten. Diese Kontrollen tragen dazu bei, die Integrität unserer Produkte während des gesamten Fertigungs-, Montage- und Lieferprozesses bis hin zur Bereitstellung zu gewährleisten. So stellen wir sicher, dass unsere Kunden genau das erhalten, was sie gekauft haben, nicht mehr und nicht weniger. Darüber hinaus geben wir diese strengen Anforderungen an alle unsere Lieferanten weiter. Im Sinne eines echten Zero-Trust-Ansatzes mit der „Annahme einer Sicherheitsverletzung", führen wir jedoch in jedem Schritt dieses Prozesses Überprüfungen durch.

Diese Überprüfungen umfassen fortschrittliche Technologien wie Secured Component Verification* zur Identifizierung von Komponententausch und SafeBIOS Off-Host-Verifizierung zur Identifizierung und Meldung von Manipulationen an der privilegiertesten Firmware im System. Diese und viele andere Funktionen sind in Dell Trusted Devices integriert, die Teil unseres Dell Trusted Workspace-Portfolios sind. Wir setzen sie jedoch auch in unserer gesamten Lieferkette ein, um alle Glieder der Kette intakt zu halten. So können wir Abweichungen erkennen, bevor sie den nächsten Schritt der Lieferkette erreichen. (*Optional erhältliche Add-on-Funktion. Die Verfügbarkeit variiert je nach Region.)

Genau das meine ich mit ergebnisorientiertem Verhalten. Diese Funktionen wurden nicht um der Innovation willen entwickelt, sondern weil sie konkrete Probleme unserer Kunden im Zusammenhang mit der Lieferkettensicherheit und dem Flottenmanagement aktiv lösen. Eben wirklich „Niemals vertrauen, immer verifizieren".

In Verbindung mit der Lieferantenbewertung sollten Sie bedenken, dass die Lieferkette Ihres OEM auch Ihre Lieferkette ist. Überprüfen Sie daher unbedingt die dortigen Praktiken. (Weitere Informationen dazu, was für die Sicherung der Lieferkette erforderlich ist, finden Sie in unserem Whitepaper zur Lieferkette.)

2. Wir entwerfen und entwickeln sichere Geräte. Hier treffen Praktiken und Funktionen aufeinander. Auf diese Weise gestalten wir effektive und innovative Hardware und Firmware.

Sicherheitsfunktionen sind heute Teil unseres marktgerechten Angebots, aber das ist nur ein Teil des Puzzles. Unsere Produkte wären nicht sicher, wenn ihr Design, ihre Entwicklung und ihre Tests nicht durch unseren verbindlichen Secure Development Lifecycle (SDL) geregelt wären. Alle Technologieanbieter müssen dafür sorgen, dass die von ihnen verkauften Produkte nicht ungewollt durch Sicherheitslücken Risiken für die NutzerInnen bergen. Um Angriffe zu verhindern und die Resilienz unseres Sicherheitssoftware-Stacks zu gewährleisten, führen wir während des Softwareentwicklungsprozesses strenge Bedrohungsmodellierungen durch, identifizieren Risiken anhand sehr komplexer Annahmen über Angreifer und wenden diese Methodik sogar auf kritische Hardware an.

Wir testen und verifizieren diese Annahmen des Bedrohungsmodells während des gesamten Entwicklungsprozesses. Dabei arbeiten wir mit einigen der besten PenetrationstestberaterInnen und externen ForscherInnen zusammen, denen wir Dell Systeme zur Verfügung stellen, um diese zu knacken. In ähnlicher Weise bieten wir ein öffentliches Bug-Bounty-Programm an, um die Sicherheit unserer kommerziellen PCs einem Stresstest zu unterziehen. Wir nehmen die Ergebnisse dieser Berichte und leiten sie an die technische Abteilung weiter, um Abhilfemaßnahmen zu entwickeln. Diesen Prozess wiederholen wir immer und immer wieder. Warum tun wir das? Die Umgebungen unserer Kunden erfordern robuste und vertrauenswürdige Geräte, um effektiv arbeiten zu können.

3. Wir sorgen dafür, dass Geräte während der Nutzung sicher sind. Sicherheit ist eine Gemeinschaftsaufgabe. Und echte Sicherheit umfasst heute den Schutz auf Hardware- und Firmwareebene sowie auf Softwareebene. Aus diesem Grund unternimmt Dell enorme Anstrengungen, um ein Ökosystem aus vollständig geprüften, erstklassigen Partnern aufzubauen, die Schutz vor Advanced Threats bieten. Viele davon sind direkt in unsere PCs integriert. Allerdings entwickeln HackerInnen ständig neue Wege, um in Software einzudringen. Aus diesem Grund sind unsere SDL-Verfahren so konzipiert, dass sie den Schutz nach der Veröffentlichung erweitern, einschließlich der Möglichkeit, Schwachstellen schnell und einfach zu identifizieren und zu beheben. Dell informiert proaktiv über bevorstehende Sicherheitsupdates und klare Sicherheitsrichtlinien, damit Kunden besser verstehen, wie ihre Produkte während ihrer gesamten Lebensdauer geschützt bleiben. Um Kunden zu helfen, Informationen zu Schwachstellen und deren Relevanz für Produktversionen schnell zu finden, haben wir alle Sicherheitshinweise und -mitteilungen an einem Ort zusammengefasst. In Kombination mit einer gut dokumentierten Richtlinie zur Reaktion auf Sicherheitslücken können wir eng mit ForscherInnen zusammenarbeiten, sobald neue Sicherheitslücken gemeldet werden. Dies verkürzt den Informationskreislauf und stellt sicher, dass stets genaue Informationen verfügbar sind, damit Kunden Risiken in ihren Umgebungen bewerten und beheben können.

Ein Sicherheitspartner, der alles zusammenbringt

Dell ist bestrebt, Vertrauen und eine sichere, vernetzte Welt zu schaffen. Wir arbeiten unermüdlich daran, Ihre Daten, Ihr Netzwerk, Ihre Organisation und Ihre Sicherheit sowie die Ihrer Kunden zu schützen, indem wir Sicherheit sorgfältig in alle unsere Lösungen integrieren. Weitere Informationen zu unseren Sicherheitspraktiken finden Sie im Dell Security and Trust Center. Bei Fragen wenden Sie sich bitte wie gewohnt an Ihre/Ihren Dell AnsprechpartnerIn oder kontaktieren Sie unsere SicherheitsspezialistInnen unter global.security.sales@dell.com

Weitere Informationen zu Dell Endpoint Security

Kontakt zu Dell Technologies ExpertInnen

Weitere Ressourcen

Diskutieren Sie mit: #HashTag

DELL Technologies