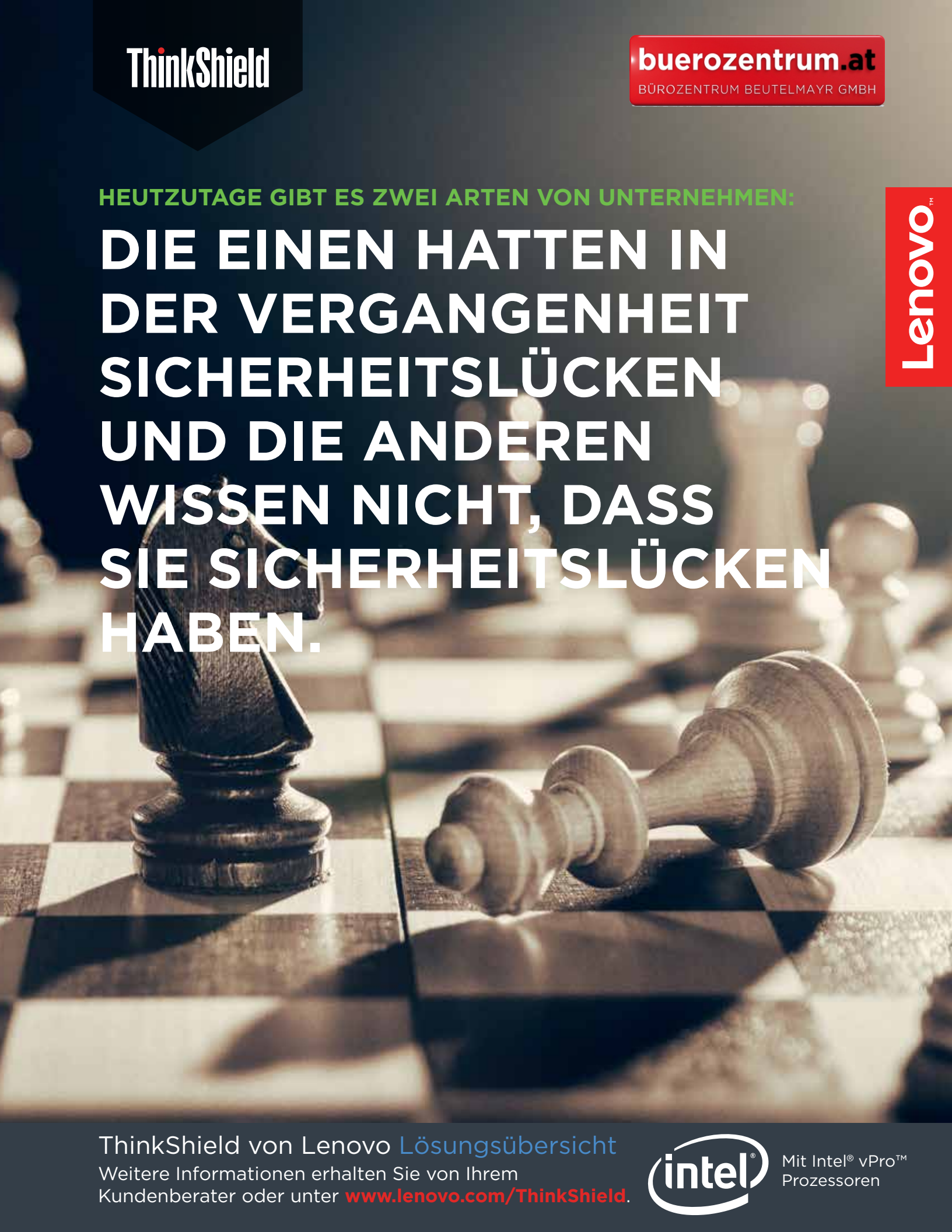

ThinkShield
buerozentrum.at
BÜROZENTRUM BEUTELMAYR GMBH
HEUTZUTAGE GIBT ES ZWEI ARTEN VON UNTERNEHMEN:
DIE EINEN HATTEN IN DER VERGANGENHEIT SICHERHEITSLÜCKEN UND DIE ANDEREN WISSEN NICHT, DASS SIE SICHERHEITSLÜCKEN HABEN.
Lenovo
ThinkShield von Lenovo Lösungsübersicht
Weitere Informationen erhalten Sie von Ihrem Kundenberater oder unter www.lenovo.com/ThinkShield.
intel
Mit Intel® vPro™ Prozessoren

2017 war das Jahr mit der höchsten Cyber-Kriminalitätsrate.

Die Zahl der Cyberangriffe steigt täglich. Und Kriminelle entwickeln immer raffiniertere und kreativere Wege, um Schwachstellen auszunutzen. 2017 erfolgte beispielsweise ein Lieferkettenangriff pro Monat, während es zuvor vier pro Jahr waren.[7] Jedes Gerät ist gefährdet, und Unternehmen müssen sich an vertrauenswürdige Technologieanbieter wenden, um den Kriminellen in Sachen Innovation zuvorzukommen.

Lenovo schützt Sie rundum.

ThinkShield von Lenovo ist die umfassendste Suite von End-to-End-Sicherheitsangeboten für Unternehmen, die derzeit auf dem Markt ist. ThinkShield ist skalierbar, um Ihre individuellen Anforderungen zu erfüllen, und umfasst Geräte-, Daten-, Identitäts- und Online-Lösungen. Damit stellen Sie sicher, dass Sie den Kriminellen immer einen Schritt voraus sind.

Lenovo ThinkShield bietet vier Schutzsäulen für Ihr Unternehmen. Geben Sie sich nicht mit weniger zufrieden.

2,6 Milliarden
Datensätze wurden kompromittiert.[1]

Phishing-Methoden im Visier
3 VON 4 Firmen.[2]

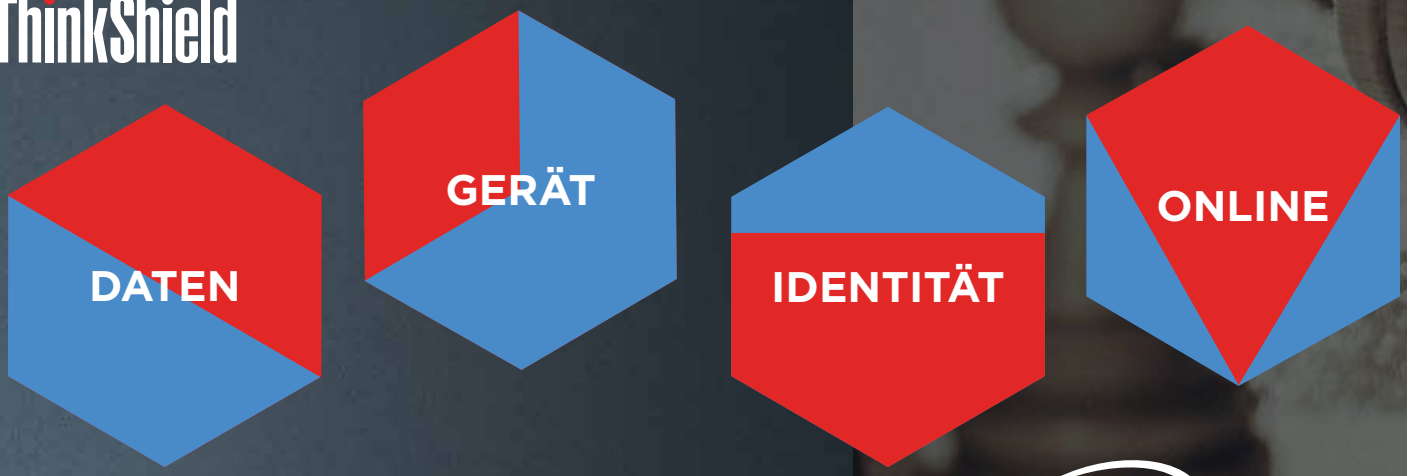
81 % der Datensicherheitsverletzungen stehen mit gestohlenen oder schwachen Kennwörtern im Zusammenhang.[3]

< 10 %
der Menschen können seriöse von bedrohlichen E-Mails unterscheiden.[4]

Datensicherheitsverletzungen kosten Unternehmen durchschnittlich
3,62 MIO. USD (3,17 MIO. EUR)[5]

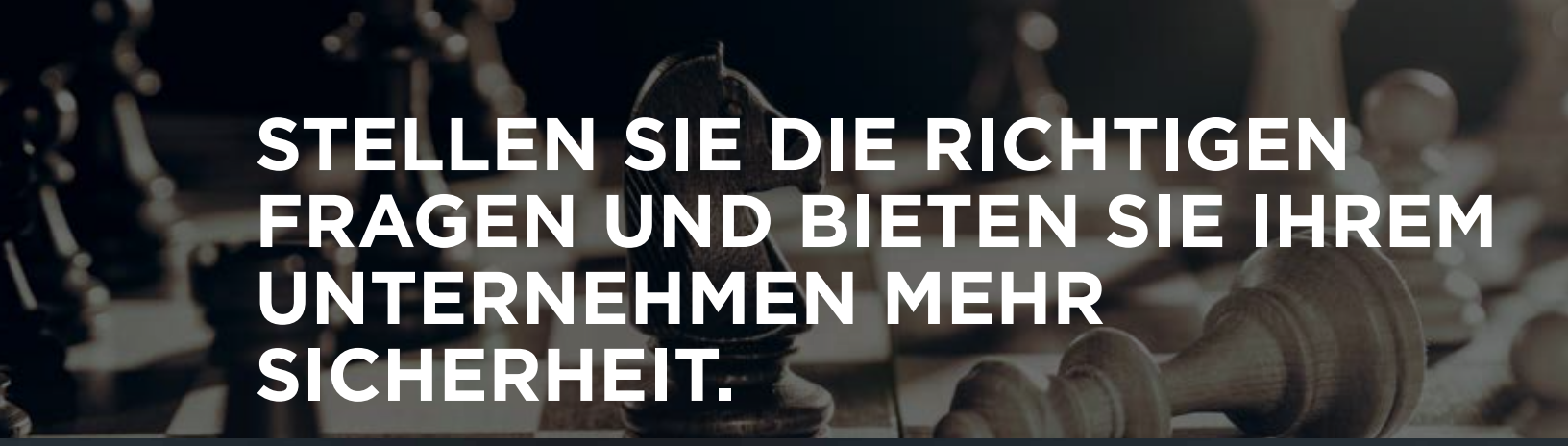
Unternehmen verloren rund
23 TAGE
durch die Behebung von Ransomware-Angriffen.[6]

ThinkShield



Weitere Informationen erhalten Sie von Ihrem Kundenberater oder unter **www.lenovo.com/ThinkShield**.

intel® Mit Intel® vPro™ Prozessoren



STELLEN SIE DIE RICHTIGEN FRAGEN UND BIETEN SIE IHREM UNTERNEHMEN MEHR SICHERHEIT.

F/A

Was bedeutet „Sicherheit durch Design" und wie wirkt sich dies auf die Sicherheit meines Unternehmens aus?

Bei Lenovo ist Sicherheit die Grundlage für alles, was wir tun. Bei der Produktentwicklung, während der Herstellung und während des gesamten Nutzungszyklus konzentrieren wir uns darauf, Bedrohungen für die Daten, die Kunden und den Ruf Ihres Unternehmens zu vermeiden.

- Zu unseren innovativen Gerätesicherheitsfunktionen zählen die ThinkShutter Kameraabdeckung, der integrierte ePrivacy-Filter und der Schutz durch Smart USB Protection.
- Die branchenweit ersten FIDO®-zertifizierten Authentifikatoren von Lenovo gewährleisten eine sicherere, kennwortfreie Benutzeranmeldung zum Schutz der Identität.
- Durch unsere Zertifizierung vertrauenswürdiger Service-Provider bleiben Ihr System, Ihre Hardware und Ihre Daten bei Reparatur und Service sicher.
- WiFi-Sicherheit mit Coronet®-Technologie und Online-Sandboxing verhindern Online-Hacking.[8]

F/A

Woher weiß ich, dass die von mir gekauften Geräte bei der Herstellung nicht kompromittiert wurden?

Sie machen sich zu Recht Sorgen. Kriminelle zielen zunehmend darauf ab, Schwachstellen in Lieferketten zu schaffen.[9] Die streng geregelte Produktlieferkette und das Trusted Supplier Program von Lenovo tragen zur Sicherheit der Geräte bei.

- Lenovo überwacht die Sicherheit von Lieferanten, die intelligente Bauteile herstellen, und sorgt dafür, dass sie unsere strengen Richtlinien und die bewährten Verfahren des Trusted Supplier Program einhalten. Für zusätzliche Transparenz können unsere Qualitätsingenieure Lieferanten jederzeit überprüfen.
- Wir arbeiten mit Intel® zusammen und passen uns an deren transparente Lieferkette an, sodass jeder Benutzer die Authentizität von PCs mit Intel Core™ vPro™ Prozessoren der 8. Generation überprüfen kann.

F/A

Wie kann ich gewährleisten, dass die sensiblen Daten meines Unternehmens auch bei weit verbreiteten Datensicherheitsverletzungen geschützt sind?

Mit ThinkShield von Lenovo sind Ihre Daten bei der Nutzung, der Wartung und am Ende der Lebensdauer von Geräten geschützt.

- Der in Lenovo ThinkPad PrivacyGuard integrierte Bildschirmfilter verhindert ein Ausspionieren über die Schulter durch Blick- und Anwesenheitserkennung.[10]
- Beim sicheren Recycling löschen wir die Laufwerke Ihrer Geräte und recyceln die Teile auf sichere Weise, sodass die Daten geschützt bleiben.
- Wenn Sie das Laufwerk eines Geräts austauschen müssen, können Sie mit unserem „Keep Your Drive"-Service (Einbehalten der Festplatte) das alte Laufwerk behalten und so gewährleisten, dass vertrauliche Informationen Ihren Arbeitsplatz niemals verlassen.[11]

Weitere Informationen erhalten Sie von Ihrem Kundenberater oder unter **www.lenovo.com/ThinkShield**.

intel®

Mit Intel® vPro™ Prozessoren

F/A

Ich befürchte, dass die Netzwerke meines Unternehmens mit Malware infiziert werden könnten. Wie kann ich gewährleisten, dass Mitarbeiter online sicher sind?

Mit innovativen Funktionen zum Schutz vor unsicheren WLAN-Netzwerken bietet Lenovo ThinkShield Lösungen, mit denen Bedrohungen erkannt und eingegrenzt werden können, bevor sie sich verbreiten.

- Lenovo WiFi-Sicherheit, mit der standardmäßig alle Lenovo Think PCs ausgestattet sind, erkennt Bedrohungen und benachrichtigt Benutzer, wenn sie eine Verbindung zu einem unsicheren Netzwerk herstellen möchten. So können Betrüger nicht auf Kennwörter und andere vertrauliche Informationen zugreifen.
- Lenovo Endpunkt-Management, unterstützt von MobileIron®, bietet eine sichere und einfache Möglichkeit, Cloud- und Endpunktsicherheit auf mehreren Geräten zu vereinheitlichen – eine ideale Sicherheitslösung für den modernen Arbeitsplatz.

Unternehmen können Daten sicher austauschen, sodass die Mitarbeiter unterwegs jederzeit und überall ihre Arbeit erledigen können. Lenovo Endpunkt-Management schützt personenbezogene Informationen (durch Erstellen einer Vertrauenszone in Bezug auf Clouds und Lenovo Geräte) und ermöglicht „Bring your own device"-Programme (indem IT-Experten Geschäftsdaten löschen können, während personenbezogene Daten erhalten bleiben). Mit dem Lenovo Endpunkt-Management können Sie sich an die Anforderungen Ihrer mobilen Mitarbeiter anpassen und dabei sicher bleiben.[12]

F/A

Wie können Mitarbeiter ihre Identität schützen, ohne Kennwörter zu verwenden, die nur schwer zu merken oder leicht zu knacken sind?

Mit Intel® Authenticate und den branchenweit ersten integrierten, FIDO®-zertifizierten Authentifikatoren blockiert ThinkShield von Lenovo Hacker aus allen Richtungen.

- Lenovo ThinkShield bietet mehrere Authentifizierungsfaktoren, viele davon werden von Intel Authenticate unterstützt. Dazu gehören Intel AMT Location, geschützte Bluetooth-Umgebung, Fingerabdruckscanner, Gesichtserkennung und geschützte PIN.
- Lenovo ist der erste Anbieter, der FIDO-zertifizierte Authentifikatoren direkt in Microsoft® Windows® PCs integriert. FIDO authentifiziert Identitäten auf Websites wie PayPal®, Google™ und Dropbox® mithilfe der sicheren Fingerabdrucktechnologie. Es ist auch eine äußerst sichere und persönliche Möglichkeit für Mitarbeiter, ihre Fingerabdrücke als zweiten Faktor zu verwenden, wenn sie sich bei Unternehmensnetzwerken und anderen verbundenen Unternehmensressourcen anmelden. Zuvor war die Implementierung dieser Art von Authentifizierung mit Risiken, Datenschutzproblemen und komplexer Verwaltung verbunden. Mit den FIDO-zertifizierten Authentifikatoren von Lenovo wird die sichere Fingerabdruck-Authentifizierung Realität.
- Unser „Match-on-Chip"-Fingerabdrucksensor verwendet die modernste Synaptics®-Technologie, um die Authentifizierung vollständig im Sensor durchzuführen und die Identitätsnachweise vor Angriffen zu schützen.
- Mit der BIOS-basierten Smart USB Protection können Sie USB-Anschlüsse so konfigurieren, dass sie nur auf Tastaturen und Zeigegeräte reagieren. Dies bedeutet, dass Ihre IT-Abteilung verhindern kann, dass Mitarbeiter Daten auf ungesicherte Geräte herunterladen, und somit Kriminelle davon abhält, die Daten Ihres Unternehmens zu stehlen.
- SmartCard-Lesegeräte bieten eine zusätzliche Sicherheitsebene für Unternehmen, die Mitarbeiterausweise zur Authentifizierung verwenden.
- Mit ThinkShutter, der integrierten Kameraabdeckung unserer neuesten Lenovo ThinkPad Notebooks, können Mitarbeiter sicherstellen, dass sie nicht beobachtet werden, wenn ihre Kameras nicht verwendet werden.

Ein Cyberangriff kommt auch auf Sie zu. Dies ist keine Zeit für Kompromisse. Mit ThinkShield von Lenovo müssen Sie auch keine eingehen.

Weitere Informationen erhalten Sie von Ihrem Ansprechpartner oder unter **www.lenovo.com/ThinkShield**.

1 https://breachlevelindex.com/assets/Breach-Level-Index-Report-2017-Gemalto.pdf
2 https://www.wombatsecurity.com/state-of-the-phish-2018
3 https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf
4 https://newsroom.intel.com/editorials/ expert-caught-phishing-net/
5,6 https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf
7 https://www.symantec.com/content/dam/symantec/ docs/reports/istr-23-executive-summary-en.pdf
8 Sandboxing ist über BUFFERZONE erhältlich, derzeit ein kostenpflichtiges Angebot in Nordamerika
9 https://www.nttsecurity.com/docs/librariesprovider3/resources/gbl-ntt-security-2018-global-threat-intelligence-report-v2-uea.pdf?sfvrsn=c761dd4d_10
10 Sowohl Anwesenheits- als auch Blickschutz erfordern ein Computermodell mit einer Infrarotkamera.
11 „Keep Your Drive" ist ein kostenpflichtiger Service. Erfahren Sie mehr unter https://www.lenovo.com/us/en/services/pc-services/lifecycle-support/warranty-protection/.
12 Lenovo Endpoint Management ist ein kostenpflichtiger Service.

Mit Intel® vPro™ Prozessoren