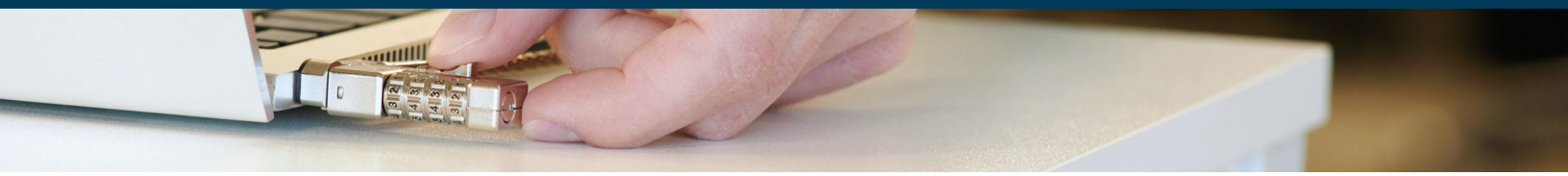
Kensington®

Gerät gesichert, Daten geschützt.

Wie physische Sicherheit dazu beitragen kann, Ihre nächste Datenschutzverletzung zu verhindern



Einleitung

Die Sicherheitssituation hat sich in den letzten Jahren dramatisch verändert, was auf den Wandel in der Art und Weise, wie und wo wir arbeiten, zurückzuführen ist. Der entscheidende Faktor war dabei die COVID-19-Pandemie; sie beschleunigte die Einführung hybrider und flexibler Arbeitsmodelle und veränderte die Prioritäten bei der Gerätesicherheit grundlegend.

Kensington unterstützte eine Studie, die vom unabhängigen Marktforschungsspezialisten Vanson Bourne durchgeführt wurde. Befragt wurden 1.000 leitende IT-Entscheidungsträger, die für die physische Hardwaresicherheit ihrer Unternehmen in den USA und der EMEA-Region verantwortlich sind. Fast alle Befragten (**92%**) verschärften ihre Sicherheitsrichtlinien als Reaktion auf die Pandemie und erkannten die erhöhten Risiken, die mit dezentralen Arbeitsumgebungen verbunden sind. Mit Blick auf das Jahr 2025 wird erwartet, dass die Zahl flexiblerer Arbeitsmodelle steigen wird, was unterstreicht, dass es jetzt an der Zeit ist, die Sicherheitsstrategien für Geräte zu überdenken.

Datenlecks sind nicht nur ein digitales Problem – jedes gestohlene oder ungesicherte Gerät stellt ein potenzielles Schlupfloch für den unbefugten Zugriff auf sensible Informationen dar und birgt erhebliche Risiken für Unternehmen. Da die finanzielle Belastung durch eine Datenschutzverletzung inzwischen im Durchschnitt Millionen von Dollar beträgt, steht mehr auf dem Spiel als je zuvor. Da Unternehmen ihre Arbeitsmodelle ständig anpassen, ist es dringend notwendig, sich mit der Gerätesicherheit zu befassen. Strengere Datenschutzanforderungen und eine Zunahme von Datenschutzverletzungen haben die Bedeutung des Schutzes sowohl physischer Geräte als auch der auf ihnen gespeicherten sensiblen Informationen weiter erhöht. Dieser Bericht hebt die entscheidende Rolle hervor, die Sicherheitsschlösser bei der Minderung dieser Risiken spielen, und unterstreicht, warum es wichtig ist, jetzt Maßnahmen zu ergreifen, um aufkommenden Herausforderungen einen Schritt voraus zu sein.

Anhand dieser Erkenntnisse werden wir die konkreten Auswirkungen von Gerätediebstählen untersuchen, aufzeigen, wie einfache, aber effektive Lösungen wie Sicherheitsschlösser dazu beitragen können, Risiken zu minimieren, und verdeutlichen, wie physische Sicherheit in einer Welt, in der sich Arbeitsmodelle ständig weiterentwickeln, für ein Gefühl der Sicherheit sorgt. Von der Veranschaulichung der erschütternden Folgen von Gerätediebstahl bis hin zum Nachweis der Kosteneffizienz und der Sicherheit von Schlössern bietet dieser Bericht umsetzbare Erkenntnisse für Organisationen, die sich in der komplexen Sicherheitslandschaft von heute zurechtfinden müssen.

Zentrale Erkenntnisse:

76% der Befragten gaben an, dass ihre Organisation in den letzten 2 Jahren von Diebstahl betroffen war, wobei Vorfälle in Unternehmen mit flexibleren Arbeitsmodellen häufiger vorkommen. Unsere Untersuchung ergab beispielsweise, dass **85%** der Unternehmen mit flexiblen Arbeitsmodellen in den letzten zwei Jahren einen Fall von Diebstahl verzeichneten, im Vergleich zu **71%** der Unternehmen, deren Mitarbeiter ausschließlich vor Ort arbeiten.

Die Auswirkungen von Gerätediebstahl gehen über den Verlust von Hardware hinaus und umfassen:

- die Notwendigkeit, bestehende Sicherheitsmaßnahmen zu verbessern (**33%**)
- rechtliche oder behördliche Konsequenzen aufgrund von kompromittierten Daten auf gestohlenen Geräten (**33%**)
- Beeinträchtigung der Mitarbeiterproduktivität durch verlorene oder gestohlene Geräte (**32%**)

Bei Unternehmen, die Sicherheitsschlösser verwenden, war die Wahrscheinlichkeit eines Datenlecks durch ein ungesichertes Gerät um **37%** geringer (**38%** gegenüber **60%** bei Organisationen, die keine Sicherheitsschlösser verwenden).

Unternehmen, die derzeit Schlösser verwenden, setzen mit größerer Wahrscheinlichkeit auch auf einen dualen Sicherheitsansatz. Drei Viertel (**76%**) verwenden digitale Maßnahmen wie Fingerabdrücke oder Sicherheitsschlüssel für die Zwei-Faktor-Authentifizierung, im Vergleich zu **62%** der Unternehmen, die überhaupt keine Schlösser verwenden.

84% stimmen zu, dass Sicherheitsschlösser bei der Eindämmung potenzieller Datenschutzverletzungen kosteneffektiv sind und einen erheblichen Mehrwert für relativ geringe Investitionen bieten.

- **42%** halten Geräteschlösser für äußerst kosteneffizient, da sie hohen Schutz zu niedrigen Kosten bieten, wobei die oberste Führungsebene ihren Wert eher erkennt (**56%**) als das mittlere Management (**36%**).

Fast alle Befragten (**97%**) glauben, dass Geräteschlösser Diebstähle verhindern und die Wahrscheinlichkeit eines unbefugten Zugriffs auf sensible Unternehmensdaten verringern können.

Gestohlene Geräte mit weitreichenden Folgen

Es vergeht kaum ein Tag, an dem Sie nicht von einem Sicherheitsvorfall hören – sei es ein groß angelegter Angriff auf ein globales Konglomerat oder eine gezieltere Manipulation kritischer Infrastrukturen oder Dienste. Und obwohl diese Beispiele zeigen, dass Cybervorfälle oft am häufigsten diskutiert werden – oder zumindest angenommen wird, dass sie es sind – ist es wichtig zu erkennen, dass physische Sicherheitsbedrohungen genauso kritisch sein können.

Es wird kaum über Vorfälle gesprochen, bei denen Unbefugte Zugang zu gesicherten Bereichen erhalten oder Vermögenswerte gefährden, was ebenso schwerwiegende Folgen hat wie ein durchschnittlicher Ransomware-Angriff. Laut unserer Umfrage geben mehr als drei Viertel (**76%**) der Befragten an, dass ihr Unternehmen in den letzten zwei Jahren von Gerätediebstählen betroffen war.

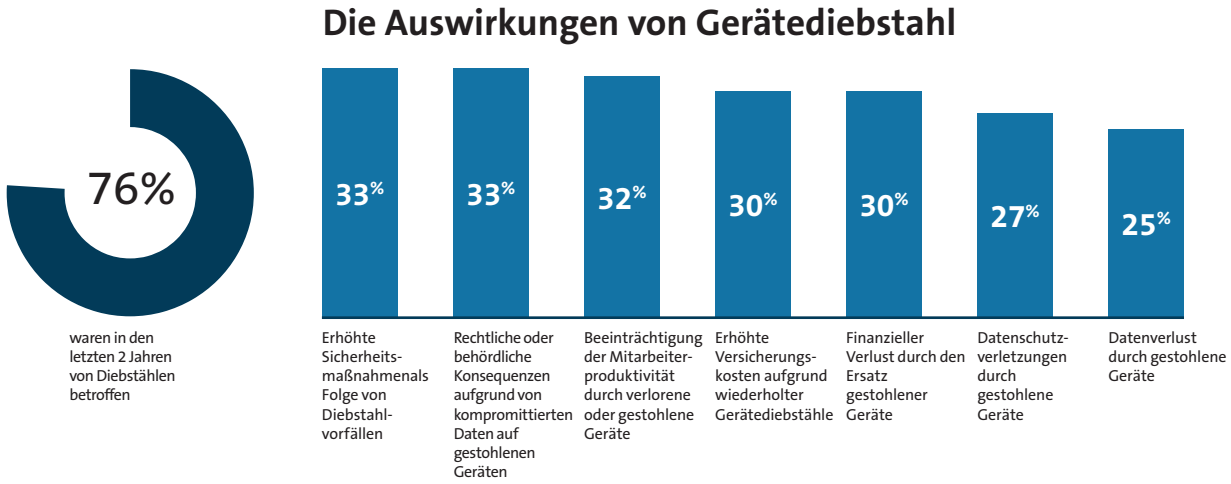


Abb. 1: *Wie hat sich der Diebstahl von Geräten in den letzten zwei Jahren auf Ihr Unternehmen ausgewirkt? [Gefragt wurden alle Teilnehmer: 1000]*

Es sind nicht nur die offensichtlichen Kosten für den Austausch eines Geräts, mit denen Unternehmen konfrontiert sind (**30%**). Zu den häufigsten Auswirkungen gehören eine Zunahme der Sicherheitsmaßnahmen, die als Folge davon eingeführt werden (**33%**), oder rechtliche oder regulatorische Konsequenzen aufgrund kompromittierter Daten (**33%**), wobei letztere oft klar umrissen sind. So können die Geldbußen der GSGVO[1] bis zu 20 Millionen Euro oder **4%** des weltweiten Umsatzes eines Unternehmens betragen, wobei selbst weniger schwerwiegende Verstöße bis zu 10 Millionen Euro kosten können, was bei Nichteinhaltung erhebliche finanzielle Risiken birgt. Zu den finanziellen Auswirkungen kommen noch die Kosten hinzu, die durch die Beeinträchtigung der Mitarbeiterproduktivität aufgrund verlorener oder gestohlener Geräte (**32%**) entstehen. Jede dieser Auswirkungen hat eindeutige finanzielle oder zeitliche Auswirkungen auf das Endergebnis des Unternehmens. Sie sehen, nicht nur digitale Sicherheitsvorfälle erfordern Aufmerksamkeit – auch physische Bedrohungen stellen ein erhebliches Risiko dar. Durch ein besseres Verständnis dieser Schwachstellen können Unternehmen einfache, kostengünstige Maßnahmen zum Schutz ihrer Geräte ergreifen. Physische Sicherheitsmaßnahmen sind sowohl erschwinglich als auch einfach umzusetzen (wie wir später noch sehen werden) und stellen einen praktischen ersten Schritt zur Stärkung der allgemeinen Sicherheit dar.

"Neben Maßnahmen zur Cybersicherheit **ist auch die physische Sicherheit gleichermaßen wichtig.** Sichere Kabel sind ein Teil einer wirksameren Strategie zu mehr Cybersicherheit."

Geschäftsführung; Fertigung und Produktion; 1.000 oder mehr Mitarbeiter; Vor-Ort-Arbeitsmodell; Frankreich

1 Bußgelder/ Sanktionen gem. DSGVO, Intersoft Consulting, https://gdpr-info.eu/issues/fines-penalties/

Heutzutage geht es nicht mehr um die Frage, ob es zu einer Datenschutzverletzung kommt, sondern wann. Tatsächlich ist jeder einzelne Gerätediebstahl eine Datenpanne, die nur darauf wartet, zu passieren, und die finanziellen Auswirkungen sind für Unternehmen verheerend. Laut dem jüngsten Bericht von IBM über die Kosten von Datenschutzverletzungen[2] liegen die weltweiten Durchschnittskosten einer Datenschutzverletzung im Jahr 2024 bei 4,88 Millionen US-Dollar; ein Anstieg von 10 % in einem Jahr gegenüber dem Durchschnitt von 4,45 Millionen US-Dollar im Jahr 2023. Diese Zahl variiert je nach Branche und Größe des Unternehmens, sodass einige Unternehmen mit noch höheren Kosten rechnen müssen.

Daten im Fokus:

- **Branchen:** Unternehmen in den Bereichen Verbraucherdienstleistungen (**95%**), Energie, Öl/Gas und Versorgungsunternehmen (**90%**) sowie Bau und Immobilien (**89%**) sind am ehesten von Gerätediebstahl betroffen. Die höhere Mobilität von Mitarbeitern und Geräten in diesen Unternehmen setzt sie einem höheren Diebstahlrisiko aus.
- **Unternehmensgröße:** Die Wahrscheinlichkeit eines Gerätediebstahls ist in kleineren Unternehmen (100–249 Mitarbeiter) stärker gestiegen (**82%**) als in größeren Unternehmen mit mehr als 1.000 Mitarbeitern (**69%**). Dies verdeutlicht die relativen Auswirkungen auf kleinere Unternehmen, in denen die Ressourcen begrenzter sind und die Auswirkungen möglicherweise stärker zum Tragen kommen.
- **Rang:** Personen in höheren Positionen geben viel häufiger an, von Diebstählen betroffen zu sein (**87%**), als Manager der mittleren Ebene (**67%**). Sie sind wahrscheinlich schlecht über die potenziellen Bedrohungen informiert, denen unsichere Geräte ausgesetzt sind. Wenn sie für die Bedrohungen und die damit verbundenen Auswirkungen sensibilisiert werden, werden Unternehmen dazu ermutigt, Sicherheitsschlösser in ihre Unternehmenskultur zu integrieren und die Perspektiven auf allen Ebenen aufeinander abzustimmen, um eine umfassende Sicherheitsstrategie zu unterstützen.

Welche Rolle spielen hier Arbeitsmodelle?

Bei der Vorstellung dieser Studie stellten wir fest, dass sich die Arbeitsweisen in den letzten Jahren grundlegend verändert haben, wobei die Einführung flexiblerer Arbeitsmodelle, die nicht mehr an einen festen Arbeitsplatz gebunden sind, durch die COVID-19-Pandemie beschleunigt wurde.

Über drei Viertel (**76%**) aller Befragten gaben an, dass ihr Unternehmen in den letzten zwei Jahren von Gerätediebstahl betroffen war. Dies wird noch deutlicher, wenn die Arbeitsmodelle flexibler sind – bei Mitarbeitern, die vollständig im Home Office arbeiten, sind es sogar über 9 von 10 (**94%**).

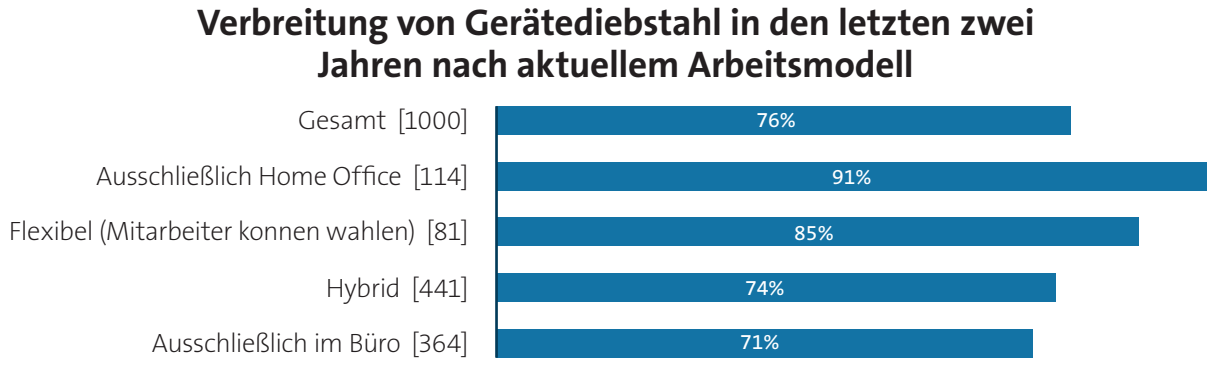


Abb. 2: *Anteil der Befragten, deren Unternehmen in den letzten zwei Jahren von Gerätediebstählen betroffen war [Befragt wurden alle Befragten, wobei die Daten nach dem aktuellen Arbeitsmodell aufgeschlüsselt sind, Basiszahlen im Diagramm]*

2 Cost of Data Breach Report 2024, IBM, July 2024, https://www.ibm.com/reports/data-breach

Während es für jedes Unternehmen wichtig ist, auf die physische Gerätesicherheit zu achten und sich der Auswirkungen von Gerätediebstahl bewusst zu sein, erhöhen flexible und ortsunabhängige Arbeitsmodelle das Risiko von Gerätediebstahl erheblich, sodass solide Sicherheitsmaßnahmen heute wichtiger denn je sind.

Sie sollten wissen, dass die Zahl der Gerätediebstähle im Allgemeinen hoch ist, selbst wenn die Mitarbeiter vollständig vor Ort sind. Unternehmen dürfen sich nicht auf ihren Lorbeeren ausruhen, unabhängig davon, wo ihre Mitarbeiter arbeiten. Die Gefahr von Gerätediebstählen ist nicht neu und auch nicht erst in dieser Welt nach der Pandemie aufgetreten. Unsere Studie aus dem Jahr 2016[3] untersuchte die Sicherheitsrisiken, die durch IT-Diebstahl in Unternehmen entstehen. Die von uns befragten Fachleute aus dem IT-Bereich stuften das Risiko eines Gerätediebstahls im Büro (**23%**) fast genauso hoch ein wie einen Diebstahl in Autos und Verkehrsmitteln (**25%**) und höher als einen Diebstahl auf Flughäfen und in Hotels (**15%**) oder Restaurants (**12%**). Hieran wird deutlich, dass der Diebstahl von Geräten auch in vollständig abgeschlossenen Umgebungen eine anhaltende Bedrohung darstellt, was die Notwendigkeit von Wachsamkeit und proaktiven physischen Sicherheitsmaßnahmen unabhängig von der Arbeitsumgebung unterstreicht.

Diese Herausforderung hat sich in der Welt nach COVID-19 noch verschärft, da **93%** der Unternehmen von einer Zunahme der Sicherheitsrisiken aufgrund der Umstellung auf flexible und hybride Arbeitsmodelle berichten. Diese Risiken gehen über den Diebstahl physischer Geräte hinaus und umfassen auch erhöhte Schwachstellen beim Datenschutz, unbefugten Zugriff und Sicherheitsverletzungen, die durch ungesicherte Heimnetzwerke und dezentrale Arbeitsumgebungen verursacht werden.

"**Es ist der einfachste Weg**, um sicherzustellen, dass unsere Geräte buchstäblich unter Verschluss sind! Es gibt uns das Gefühl, dass **alles sicher und geschützt ist.**"

Vorstandsmitglied/C-Level; IT, Technologie und Telekommunikation; 100–249 Mitarbeiter; flexibles Arbeitsmodell; USA

Vor diesem Hintergrund besteht der beste Sicherheitsansatz darin, robuste physische Maßnahmen

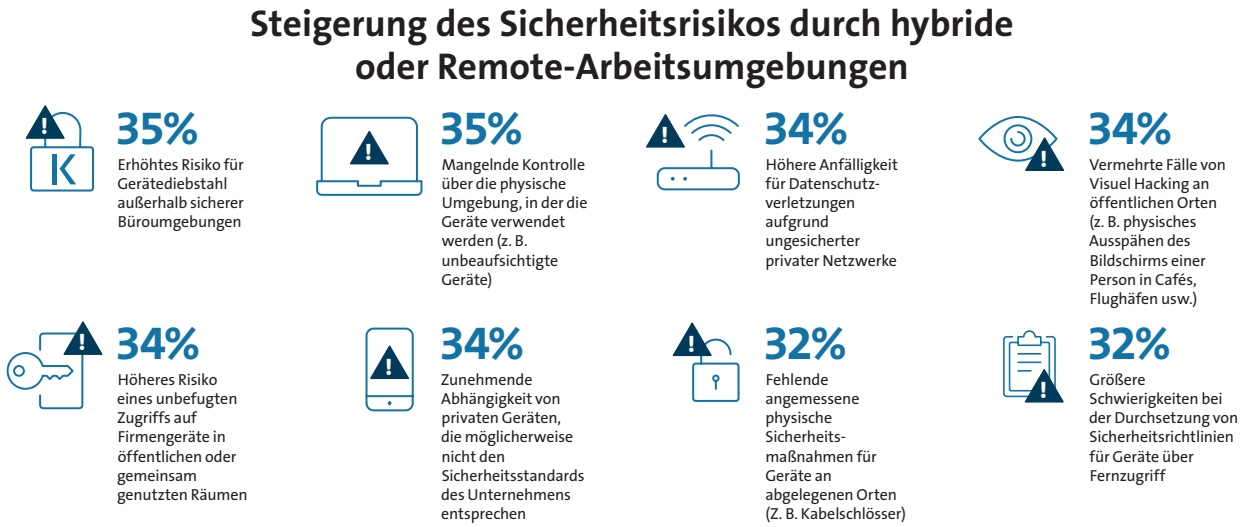


Abb. 3: *Welche Sicherheitsrisiken haben sich Ihrer Meinung nach durch hybride oder mobile Arbeitsumgebungen infolge der COVID-19-Pandemie erhöht? [Befragt wurden Personen, deren Unternehmen nach der COVID-19-Pandemie auf hybride/mobile Arbeit umgestellt hat: 494]*

mit fortschrittlichen digitalen Sicherheitsvorkehrungen zu kombinieren, um in einer zunehmend dezentralisierten Welt einen umfassenden Schutz für Geräte und Daten zu gewährleisten.

3 IT Security & Laptop Theft Survey, Kensington, August 2016, https://www.kensington.com/news/news-press-center/2016-news--press-center/kensington-survey-data-reveals-that-it-theft-in-the-office-ranks-nearly-as-high-as-theft-in-cars-and-more-than-in-airports-or-restaurants/?srsltid=AfmBOooRTMdZ4gjmcNB3viXIJcIL4GY47XxO5I08AldLhLEB5LjnH0Ts

Schlösser, die Verluste verhindern – und Kosten sparen

"Das Fehlen eines Sicherheitsschlosses bei der Ausrüstung führte zu einer Datenschutzverletzung, die dem **Unternehmen erhebliche Verluste bescherte.**"

Mittlere Führungsebene; IT, Technologie und Telekommunikation; 1.000 oder mehr Mitarbeiter; flexibles Arbeitsmodell; USA

Bisher haben wir die Folgen von Gerätediebstahl aufgedeckt und gezeigt, wie weit verbreitet dies unabhängig vom Arbeitsumfeld sein kann. Dies ist jedoch nicht das einzige Anliegen unserer befragten leitenden IT-Entscheidungsträger. Sie machen sich in Bezug auf die Sicherheit sowohl in physischen als auch in digitalen Bereichen über eine Vielzahl von Aspekten Sorgen.

Einige dieser Bedenken betreffen neuere Faktoren im Zusammenhang mit der physischen Sicherheit. Zum Beispiel ist fast ein Viertel (**23%**) besorgt über Visual Hacking, bei dem sensible Daten jedem ausgeliefert sind, wenn jemandes Bildschirm an einem öffentlichen Ort – in einem Café oder in öffentlichen Verkehrsmitteln – zu sehen ist. Tatsächlich berichten diejenigen, die flexibel arbeiten (**48%**), häufiger als diejenigen, die ausschließlich im Home Office (**36%**) oder in einer hybriden Arbeitsumgebung (**33%**) arbeiten, dass sie sich Sorgen über visuelles Hacking machen. Dies zeigt, dass visuelles Hacking nicht nur mit der Arbeit von zu Hause aus verbunden ist, sondern auch mit der Gewährung übermäßiger Freiheiten, die schwieriger zu kontrollieren sind. Unternehmen müssen den Schutz ihrer Daten berücksichtigen, wenn Mitarbeiter unterwegs sind, und zusätzliche Abschreckungsmaßnahmen wie Blickschutzfilter einsetzen.

Die problematischsten Bereiche der Gerätesicherheit

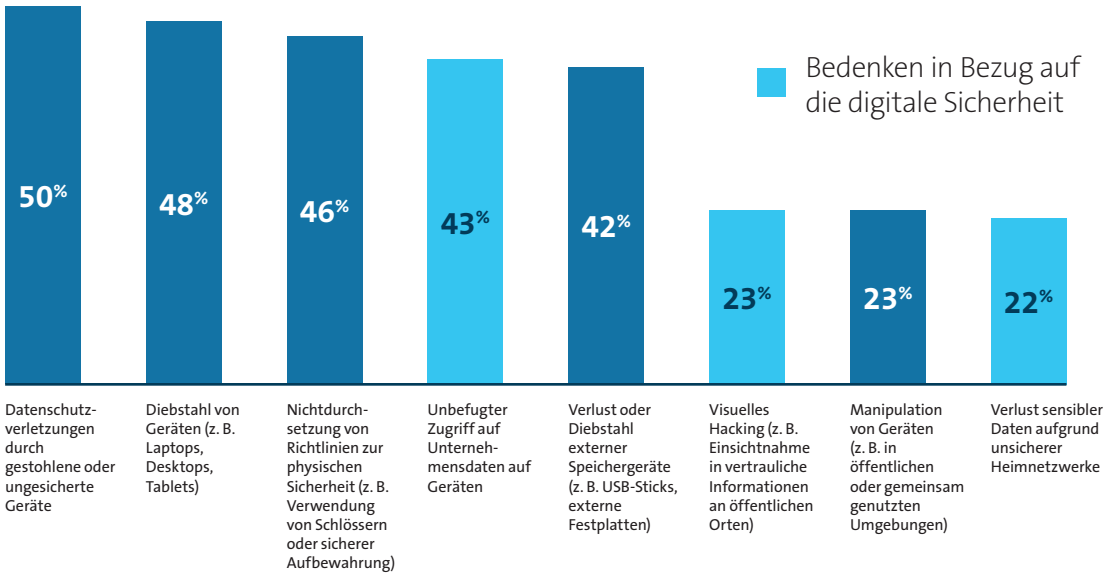


Abb. 4: *Welche Bereiche der Gerätesicherheit in Ihrem Unternehmen bereiten Ihnen die größten Sorgen? [An alle Befragten: 1000, wobei die Kombination der Antworten an erster, zweiter und dritter Stelle angezeigt wird]*

Datenschutzverletzungen sind jedoch das größte Problem, was durchaus begründet ist, da ein beträchtlicher Anteil (**46%**) bereits eine Datenschutzverletzung als direkte Folge eines ungesicherten Geräts erlebt hat.

Hier kann ein Sicherheitsschloss helfen. Bei Unternehmen, die Sicherheitsschlösser verwenden, ist die Wahrscheinlichkeit einer Datenschutzverletzung aufgrund eines ungesicherten Geräts um **37%** geringer als bei Unternehmen, die überhaupt keine Sicherheitsschlösser verwenden.

Unternehmen, die aufgrund eines ungesicherten Geräts eine Datenpanne oder den Verlust sensibler Daten erlebt haben

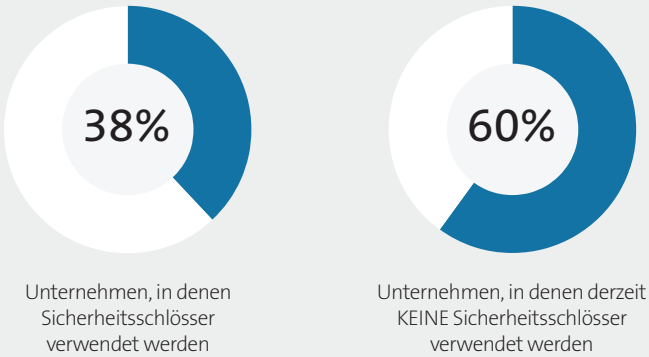


Abb. 5: *Hat Ihr Unternehmen bereits eine Datenschutzverletzung oder den Verlust sensibler Daten als direkte Folge eines ungesicherten Geräts erlebt? [Frage an alle Befragten, aufgeteilt nach denjenigen, die derzeit Sicherheitsschlösser verwenden: 629; und diejenigen, die derzeit keine Sicherheitsschlösser verwenden: 371]*

Das Ergebnis ist eindeutig: Eine messbare Reduzierung von Datenschutzverletzungen oder Datenverlusten unterstreicht den Wert von Sicherheitsschlössern als entscheidende Komponente eines umfassenden Geräteschutzes. Diese überzeugenden Beweise zeigen, wie Sicherheitsschlösser Risiken direkt mindern und sie zu einer wesentlichen Investition für Unternehmen machen, die sich für den Schutz ihrer Daten und die Minimierung von Sicherheitslücken einsetzen.

Daten im Fokus:

- **Branche:** Laut Umfrageergebnissen sind Unternehmen in den Bereichen Verbraucherdienstleistungen (**65%**) und öffentliches/privates Gesundheitswesen (**57%**) eher von einer Datenpanne betroffen, die auf ein ungesichertes Gerät zurückzuführen ist. Ersteres war am ehesten von Gerätediebstahl im Allgemeinen betroffen. Bei Letzterem wirft dies möglicherweise größere Bedenken hinsichtlich der dezentralen Natur von Gesundheitseinrichtungen und des engeren Kontakts der Öffentlichkeit mit Geräten auf. Die Fülle an sensiblen Daten in dieser Branche stellt ein erhöhtes Risiko dar
- **Unternehmensgröße:** Kleinere Unternehmen sind aufgrund ihrer begrenzten Ressourcen eher (**59%**) als größere Unternehmen (**40%**) von einem Datenleck aufgrund eines ungesicherten Geräts betroffen. Sie haben nicht nur mit den primären Abschreckungsmaßnahmen zu kämpfen, sondern auch mit dem Schneeballeffekt, der folgt.
- **Rang:** Die jüngeren der Befragten melden mit geringerer Wahrscheinlichkeit einen Datenverstoß oder den Verlust sensibler Daten aufgrund eines ungesicherten Geräts (**30%**) als ihre Kollegen in der Geschäftsführung/im Vorstand (**59%**). Es gibt eine klare Fehlausrichtung innerhalb von Unternehmen, wenn es um ein echtes Verständnis der Sicherheit physischer Geräte und die Folgen geht, wenn diese nicht vorhanden ist – ein Aufruf zu umfassenderer Bildung und zum Wissensaustausch.

"Eine geringe Anfangsinvestition in Sicherheitsmaßnahmen (Schlösser) kann die **Wahrscheinlichkeit kostspieliger Geräteerneuerungen oder längerer Ausfallzeiten erheblich verringern.**"

Geschäftsleitung; Bildung – staatlich/staatlich bereitgestellt; 1.000 oder mehr Mitarbeiter; Hybrides Arbeitsmodell; USA

Wie sollten Unternehmen also vorgehen, um dieses Problem zu lösen?

Unternehmen sind mit so vielen digitalen und physischen Sicherheitsbedenken konfrontiert, und die Auswirkungen von Gerätediebstählen sind für Unternehmen und ihre Bilanzen verheerend. Sie sollten nach der kostengünstigsten Lösung suchen. Aufgrund ihres nachweislichen Erfolgs könnten ein einfaches Sicherheitsschloss ausreichen.

Die Mehrheit (**84%**) unserer befragten leitenden IT-Entscheidungsträger gibt an, dass Sicherheitsschlösser bei der Eindämmung potenzieller Datenschutzverletzungen kosteneffektiv sind – dass sie einen erheblichen Mehrwert bei der Verhinderung von Diebstahl und Verstößen bieten. Darüber hinaus glauben **42%**, dass sie äußerst kosteneffizient sind.

Diese Meinung wird von allen geteilt, die bereits Sicherheitsschlösser verwenden, und sogar von denen, die dies nicht tun – was die Frage aufwirft, warum nicht? Unternehmen könnten Schlösser als logistische Herausforderung für die Geräteverwaltung betrachten oder vielleicht führt eine stärkere Fokussierung auf digitale statt physische Sicherheit dazu, dass der Wert von Schlössern unterschätzt wird, was wiederum die Akzeptanz behindert. Verglichen mit den enormen finanziellen Folgen eines Gerätediebstahls stellen die Kosten für ein Sicherheitsschloss – in der Regel durchschnittlich nur 30 bis 50 US-Dollar pro Gerät – jedoch eine minimale Investition zur Risikominderung dar. Wenn wir uns näher damit befassen, sehen wir einen klaren Meinungsunterschied in der Organisationshierarchie.

Einschätzung der Kosteneffizienz von Sicherheitsschlössern

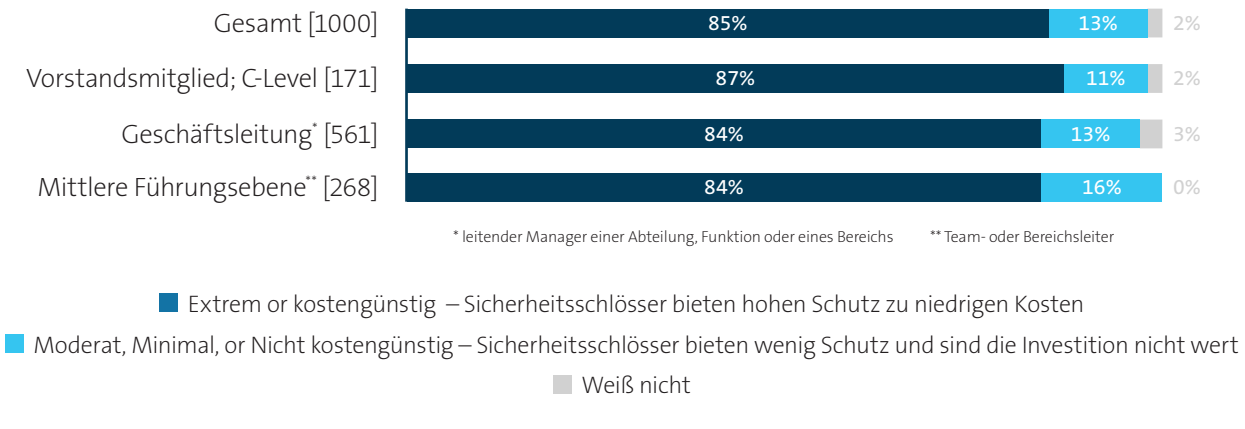


Abb. 6: *Wie sehen Sie die Rolle von physischen Sicherheitsschlössern in Bezug auf die Kosteneffizienz bei der Eindämmung potenzieller Datenschutzverletzungen oder Diebstähle? [Frage an alle Befragten, Daten nach Dienstalter aufgeschlüsselt, Basiszahlen im Diagramm]*

Diese Ergebnisse unterstreichen die dringende Notwendigkeit, die Ursachen von Gerätediebstählen und ihre weitreichenden Auswirkungen auf ein Unternehmen anzugehen. [Diagramm] Während Führungskräfte in höheren Positionen Sicherheitsschlösser eher als äußerst kosteneffizient ansehen (**56%**), nimmt diese Überzeugung auf den unteren Hierarchieebenen ab. Letztendlich werden sich Führungskräfte immer mehr auf die weiterreichenden Auswirkungen (z. B. Bußgelder, Rufschädigung) konzentrieren, während Manager auf niedrigerer Ebene sich auf die täglichen Auswirkungen (z. B. Produktivitätsverlust) konzentrieren.

Diese Diskrepanz unterstreicht, wie wichtig die organisatorische Abstimmung und die Aufklärung über den Wert von Sicherheitsschlössern ist – nicht nur als kostengünstiges Werkzeug, sondern als proaktive Lösung, um erhebliche Verluste zu verhindern, bevor sie entstehen. Durch die Überbrückung dieser Wahrnehmungslücken wird ein einheitlicher und wirksamer Ansatz zur Minderung der Risiken von Gerätediebstahl und zum Schutz sensibler Daten gewährleistet.

> "Einmal verloren, wird es erhebliche Verluste verursachen. Wir müssen **das Problem an der Wurzel packen.**"

Mittlere Führungsebene; Gesundheitswesen – in Privatbesitz; 1.000 oder mehr Mitarbeiter; Hybrides Arbeitsmodell; USA.

Schlösser dienen der Sicherheit und schaffen Vertrauen

Wir haben weiter untersucht, wie Sicherheitsschlösser nicht nur Diebstahl wirksam reduzieren, sondern auch eine kostengünstige Lösung zur Minderung allgemeiner Sicherheitsrisiken bieten. Ihre vielfältigen Einsatzmöglichkeiten unterstreichen ihre Vielseitigkeit bei der Bewältigung von Sicherheitsherausforderungen in verschiedenen Umgebungen – ein Vorteil, den viele Unternehmen bereits erkannt haben.

Viele verwenden bereits Sicherheitsschlösser, um elektronische Geräte in ihrem Unternehmen zu sichern. Zu den am häufigsten gesicherten Geräten gehören Laptops (**44%**), Desktop-PCs (**43%**) und Server (**42%**), was die Priorität widerspiegelt, die dem Schutz kritischer Hardware beigemessen wird, die oft sensible Daten enthält. Diese weit verbreitete Anwendung unterstreicht die Anerkennung von Schlössern als wichtiges Instrument zum Schutz vor Diebstahl und unbefugtem Zugriff.

Einschätzung der Kosteneffizienz von Sicherheitsschlössern

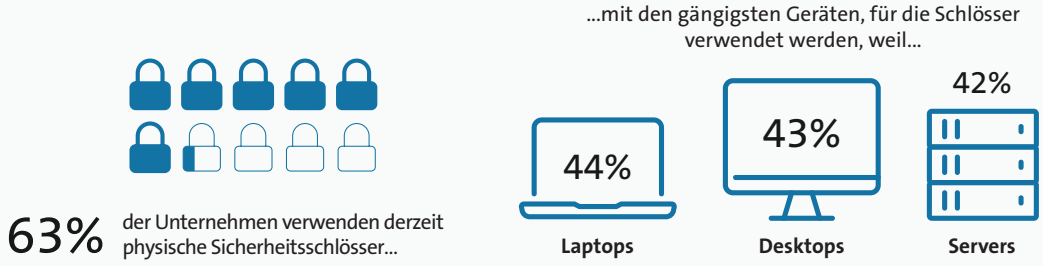


Abb. 7: *Für welche der folgenden elektronischen Geräte werden in Ihrem Unternehmen physische Sicherheitsschlösser verwendet? [An alle Befragten: 1000]*

Die Tatsache, dass fast 4 von 10 Befragten angeben, dass ihre Unternehmen keine Schlösser verwenden, wirft jedoch Bedenken hinsichtlich der Schwachstellen in den Sicherheitsstrategien für Geräte auf, insbesondere bei Geräten, die häufig in mobilen oder hybriden Arbeitsumgebungen eingesetzt werden.

Für Unternehmen unterstreichen diese Daten die Notwendigkeit, ihre aktuellen Sicherheitsmaßnahmen umfassend zu bewerten. Obwohl Schlösser eine bewährte und weit verbreitete Lösung sind, kann eine Ausweitung ihrer Verwendung auf eine breitere Palette von Geräten und die Kombination mit ergänzenden digitalen Schutzmaßnahmen dazu beitragen, bestehende Sicherheitslücken zu schließen und Risiken wirksamer zu mindern.

Fast alle Befragten (**97%**) erkennen die entscheidende Rolle an, die Sicherheitsschlösser bei der Verhinderung von Diebstahl und dem damit oft verbundenen unbefugten Zutritt spielen. Diese weit verbreitete Anerkennung spiegelt das Vertrauen wider, das Unternehmen in die physische Sicherheit als grundlegende Maßnahme zum Schutz von Geräten und sensiblen Daten setzen. Schlösser dienen als erste Sicherheitsbarriere, indem sie die Gelegenheiten für Diebstahl verringern und die Risiken im Zusammenhang mit manipulierter Hardware mindern.

"Schlösser in Großraumbüros, Gemeinschaftsbüros oder anderen Bereichen, in denen sich mehrere Personen aufhalten können, **verringern das Diebstahlrisiko.**"

Vorstandsmitglied/C-Level; Bildung – in Privatbesitz; 100–249 Mitarbeiter; USA

Überzeugung, dass physische Sicherheitsmaßnahmen zur Verhinderung von Gerätediebstahl beitragen

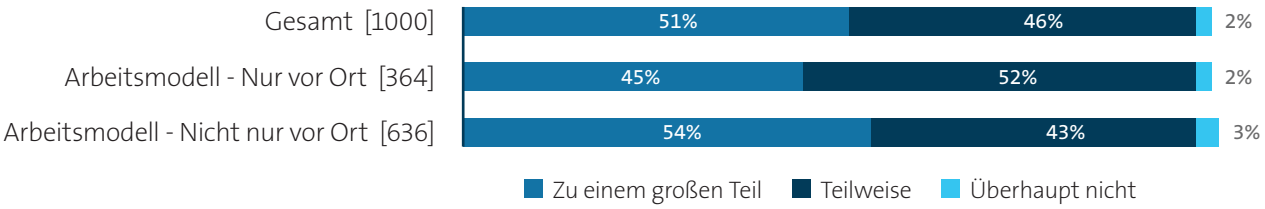


Abb. 8: *Inwieweit glauben Sie, dass physische Sicherheitsmaßnahmen wie Sicherheitsschlösser dazu beitragen, Gerätediebstahl zu verhindern, der zu einem unbefugten Zugriff auf Unternehmensdaten führen könnte? [An alle Befragten, Daten nach Art des Arbeitsmodells aufgeschlüsselt, Basiszahlen im Diagramm]*

Diese Erkenntnis gewinnt an Bedeutung, wenn Unternehmen flexible und hybride Arbeitsmodelle einführen. In diesen dezentralen Umgebungen werden Geräte zunehmend an ungesicherten Orten wie Home Offices oder öffentlichen Räumen verwendet, was das Risiko von Diebstahl oder versehentlicher Offenlegung erhöht. Datenverletzungen, die durch ungesicherte Geräte verursacht werden, treten in flexibleren Arbeitsumgebungen deutlich häufiger auf (**50%** insgesamt gegenüber **39%** bei einem Vor-Ort-Arbeitsmodell).

Sicherheitsschlösser sind so konzipiert, dass sie sich an unterschiedliche Umgebungen anpassen und einen zuverlässigen Schutz für Geräte bieten, unabhängig davon, ob sie in Büros, an entfernten Arbeitsplätzen oder in öffentlichen Einrichtungen verwendet werden. So können Unternehmen bei allen Arbeitsmodellen beruhigt sein.

Die finanziellen Folgen eines Gerätediebstahls können verheerend sein, wobei die Kosten für den Ersatz gestohlener Hardware oft in den Schatten gestellt werden durch die umfassenderen Auswirkungen auf die Produktivität, die Einhaltung von Vorschriften und Datenschutzverletzungen. Für Unternehmen erhöht jedes gestohlene oder ungesicherte Gerät das Risiko – nicht nur für den Betrieb, sondern auch für das Endergebnis. Sicherheitsschlösser sind eine bewährte und kostengünstige Lösung, der viele bereits vertrauen, um die Wahrscheinlichkeit eines Diebstahls und die daraus resultierenden finanziellen und rufschädigenden Folgen zu verringern. Indem Unternehmen diese Risiken an der Wurzel angehen, können sie proaktiv handeln, um ihre Vermögenswerte und sensiblen Daten zu schützen.

Physische Sicherheitsmaßnahmen wie Schlösser sind zwar wirksam, müssen aber Teil einer umfassenderen Strategie sein, um den sich entwickelnden Sicherheitsrisiken im Zusammenhang mit hybrider Arbeit zu begegnen. Die Kombination von Schlössern mit ergänzenden digitalen Schutzmaßnahmen wie Verschlüsselung und Zwei-Faktor-Authentifizierung gewährleistet einen umfassenden Schutz vor physischen und digitalen Bedrohungen. Schulungsprogramme, die Mitarbeiter über die Bedeutung dieses integrierten Ansatzes aufklären, können die Sicherheit in Organisationen weiter stärken. Für Unternehmen, die sich in der Komplexität moderner Arbeitsmodelle zurechtfinden müssen, ist die Integration physischer und digitaler Sicherheitsmaßnahmen unerlässlich, um Risiken zu minimieren, ihre Belegschaft zu schützen und die betriebliche Widerstandsfähigkeit aufrechtzuerhalten.

Es ist weitaus kostengünstiger, Gerätediebstähle und die daraus resultierenden Datenschutzverletzungen zu verhindern, als die Folgen zu bewältigen. Präventivmaßnahmen wie die Verwendung von Laptopschlössern können Ihr Unternehmen heute vor erheblichen finanziellen und betrieblichen Auswirkungen in der Zukunft schützen. Um sicherzustellen, dass diese Maßnahmen wirksam sind, ist eine Abstimmung zwischen der obersten Führungsebene, dem Management und den Teams von entscheidender Bedeutung. Ein gemeinsames Engagement für Sicherheitsprioritäten stellt sicher, dass jeder seine Rolle beim Schutz wertvoller Vermögenswerte und bei der Risikominderung versteht.

Methodik

Kensington beauftragte den unabhängigen Marktforschungsspezialisten Vanson Bourne mit der Durchführung der Studie, auf der dieser Bericht basiert. Insgesamt wurden im Herbst 2024 1.000 leitende IT-Führungskräfte, die in ihren Unternehmen für die physische Sicherheit von IT-Hardware zuständig sind oder Einfluss darauf haben, befragt. Die Befragten kamen aus den USA, Großbritannien, Frankreich und Deutschland.

Die Befragten mussten aus Unternehmen mit 100 oder mehr Mitarbeitern und aus verschiedenen privaten und öffentlichen Sektoren stammen.

Die Interviews wurden online durchgeführt und unter Anwendung eines strengen mehrstufigen Auswahlverfahrens durchgeführt, um sicherzustellen, dass nur geeignete Kandidaten die Möglichkeit zur Teilnahme erhielten. Sofern nicht anders angegeben, basieren die besprochenen Ergebnisse auf der Gesamtstichprobe.

Über Kensington

Kensington ist ein führender Anbieter von Zubehör für Desktops und Mobilgeräte, dem IT-Fachleute, Bildungseinrichtungen, Unternehmen und professionelle Anwender im Home Office auf der ganzen Welt seit mehr als 40 Jahren vertrauen. Kensington ist stets bestrebt, die Bedürfnisse und Herausforderungen der sich ständig weiterentwickelnden Arbeitswelt zu antizipieren und ausgezeichnete Lösungen für Unternehmen zu entwickeln, die ihren Mitarbeitern die notwendigen Tools an die Hand geben wollen, um erfolgreich zu sein. Das Unternehmen ist stolz darauf, die erste Wahl für professionelle Anwender zu sein, und auf seine Kernwerte rund um Design, Qualität und Support.

In Büro- und mobilen Umgebungen bietet Kensington ein umfangreiches Portfolio an ausgezeichneten Produkten für zuverlässige Sicherheit, innovative Desktop-Produktivität, professionelle Videokonferenzen und ergonomisches Wohlbefinden.

Kensington ist als Erfinder und Anbieter von Sicherheitsschlössern für Laptops weltweit führend. Der Hauptsitz des Unternehmens befindet sich in Burlingame, Kalifornien. Kensington ist ein Geschäftsbereich von ACCO Brands, der Heimat von großartigen Marken, die von großartigen Menschen geschaffen wurden. ACCO Brands entwickelt, produziert und vermarktet Produkte, die den Menschen helfen, zu arbeiten, zu lernen, und zu spielen. Neben Kensington® gehören zu den weithin anerkannten Marken von ACCO Brands auch AT-A-GLANCE®, Five Star®, Leitz®, Mead®, PowerA®, Swingline®, Tilibra und viele andere. Weitere Informationen über ACCO Brands Corporation (NYSE:ACCO) finden Sie unter www.accobrands.com.

FOR MORE INFORMATION CONTACT: sales@kensington.com