2019 UNISYS SECURITY INDEX™

GERMANY REPORT

UNISYS | Securing Your Tomorrow®

Zusammenfassung Deutschland

Der Unisys Security Index™ zeigt, dass die Deutschen gar nicht so besorgt um ihre Sicherheit sind, wie es oft den Anschein haben mag. Tatsächlich sind die Sicherheitsbedenken in Deutschland das dritte Jahr in Folge zurückgegangen. Populäre Stereotypen bezüglich einer sprichwörtlichen „German Angst“ treffen also in Wahrheit nicht zu, wenn es um die Wahrnehmung der eigenen Sicherheit in Deutschland geht.

Der Unisys Security Index in Deutschland ist seit 2017 stetig gesunken und rangiert nun bei 123 von 300 möglichen Punkten im Jahr 2019. Nach den Niederlanden, die den niedrigsten Wert halten, liegt Deutschland damit weltweit auf dem zweitniedrigsten Rang des Unisys Security Index bezüglich Sicherheitsbedenken. Der globale Durchschnitt liegt bei 175 Punkten.

Deutschland positioniert sich aktuell als treibende Kraft für „Smart Cities“-Initiativen und hat in den vergangenen fünf Jahren Milliarden von Dollar in entsprechende Forschung und Technologie investiert. Die deutschen Bürger scheinen jedoch nur ein vages Verständnis für „Smart City“-Konzepte zu haben – und die Entwicklung von smarten Städten hat zu neuen Bedenken geführt: So sind fast drei Viertel (71%) der Deutschen ernsthaft besorgt über „Smart City“-Initiativen und die damit verbundenen Technologien.

Insbesondere machen sich die Deutschen Gedanken über Sicherheitsbedrohungen durch die Nutzung privater Drohnen und durch autonomes Fahren. Sogar die Befragten, die eigentlich offen für Entwicklungen und Trends in diesen Technologien sind, zeigen sich zumindest etwas ängstlich.

Konkret geben 56% der Deutschen an, dass sie nicht möchten, dass private Eigentümer Drohnen einsetzen; 31% der Deutschen geben an, dass sie sich auf autonome Fahrzeuge nicht verlassen würden.

Die Teilnahme an Großveranstaltungen wie einer Weltmeisterschaft oder einem großen Musikfestival ist für die Deutschen eine weitere Quelle für Sicherheitsbedenken.

Die Möglichkeit des Diebstahls personenbezogener Daten und potenzielle Gefahren für die physische Sicherheit haben ein Viertel (25%) der Deutschen schon einmal veranlasst, über die Teilnahme an Großveranstaltungen zweimal nachzudenken. Tatsächlich haben 16% ihre Pläne zur Teilnahme an bestimmten Veranstaltungen aufgrund von Sicherheitsbedenken bereits einmal geändert. Und selbst wenn 52% der Deutschen ihre Pläne nicht ändern würden, geben viele an, doch zusätzliche Vorsichtsmaßnahmen treffen – indem sie etwa mobile Geräte und Brieftaschen sichern.

©2019 Unisys Corporation. Alle Rechte vorbehalten.

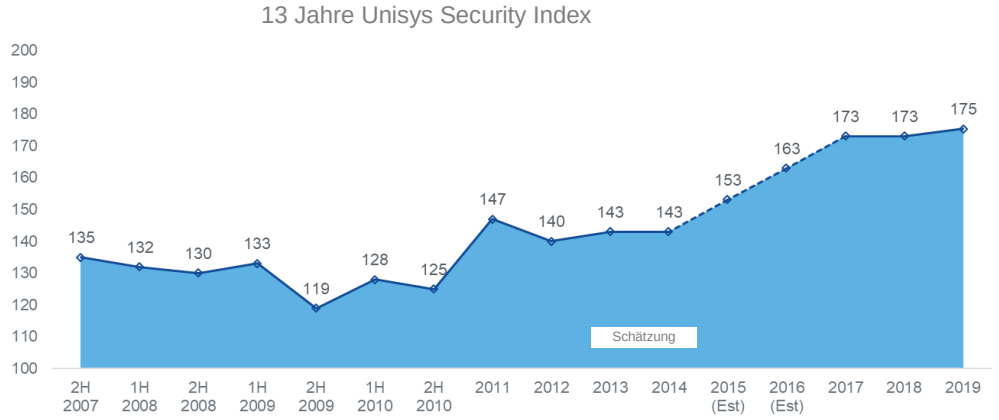
Globale Zusammenfassung

Der Unisys Security Index verfolgt seit mehr als einem Jahrzehnt Sicherheitsbedenken auf der ganzen Welt und stellt fest, dass diese Bedenken in den letzten fünf Jahren erheblich zugenommen haben. In diesem Jahr wurde das Niveau an Bedenken auf dem höchsten Stand seit Beginn der Umfrage im Jahr 2007 gemessen.

Der Unisys Security Index für 2019 liegt weltweit bei 175 (von 300), ein Anstieg um 2 Punkte seit 2018. Zum dritten Mal in Folge sind Identitätsdiebstahl und Kreditkartenbetrug die beiden größten Befürchtungen weltweit. Identitätsdiebstahl steht weiterhin an der Spitze der acht im Index abgefragten Unsicherheits-Szenarien, und mehr als zwei Drittel der Befragten (69%) geben hier ernsthafte Sorgen an. Diese Besorgnis übersteigt sogar die Angst vor Krieg, Terrorismus oder Naturkatastrophen. Möglicher Betrug mit Bankkarten gehört ebenfalls zu den beiden größten Sicherheitsbedenken weltweit: Zwei Drittel (66%) der Verbraucher sind ernsthaft besorgt darüber.

Auch zunehmende Sicherheitsbedenken bei Internet-Aktivitäten prägen den diesjährigen Unisys Security Index. Fast zwei Drittel (63%) der Verbraucher geben an, ernsthaft besorgt über Bedrohungen durch Viren oder Hacking zu sein. Und mehr als die Hälfte der Befragten (57%) macht sich ernsthafte Sorgen bei Online-Shopping und -Banking.

Im Allgemeinen sind Verbraucher in Entwicklungsländern besorgter als in Industrieländern. Die Verbraucher auf den Philippinen zeigen die höchsten Sicherheitsbedenken der 13 untersuchten Länder, die Verbraucher in den Niederlanden die niedrigsten – obwohl auch ihre Besorgnis zunimmt. Jüngere Befragte und Personen mit geringerem Einkommen haben alles in Allem höhere Sicherheitsbedenken.



Die Umfrage wurde 2019 um eine Perspektive erweitert: nämlich um Bedenken, die Verbraucher haben, wenn sie an Großveranstaltungen wie einer Weltmeisterschaft oder großen Musikfestivals teilnehmen. Nach einigen schweren Vorfällen auf der ganzen Welt im vergangenen Jahr stellte die Umfrage zum Unisys Security Index fest, dass die globalen Sicherheitsbedenken der Verbraucher hinsichtlich der Teilnahme an solchen Veranstaltungen hoch sind.

Interessanterweise gaben die Verbraucher an, dass sie bei Großveranstaltungen genauso besorgt um ihre persönlichen Daten sind wie um ihre körperliche Unversehrtheit: 57% der Befragten in den 13 befragten Ländern gaben an, ernsthafte („extreme“, bzw. „große“) Bedenken hinsichtlich eines physischen Angriffs bei einem Großereignis zu haben – ebenso viele zeigen sich besorgt, dass ihre persönlichen Daten, etwa bei der Nutzung von öffentlichem WLAN, kompromittiert werden könnten. 59% äußerten ernsthafte Bedenken, dass ihre Kreditkartendaten gestohlen werden könnten.

28% der Befragten haben ihre Pläne zur Teilnahme an bestimmten Großveranstaltungen bereits einmal aufgrund von Sicherheitsbedenken geändert, und fast vier von zehn Befragten (39%) sagten, sie würden zweimal überlegen, ob sie an solchen Veranstaltungen teilnehmen möchten. Auch ein Viertel derjenigen, die ihre Pläne nicht ändern, gibt jedoch an, zusätzliche Vorsichtsmaßnahmen zur Sicherung mobiler Geräte und Brieftaschen zu treffen.

©2019 Unisys Corporation. Alle Rechte vorbehalten.

Der Unisys Security Index: 13 Jahre und mehr

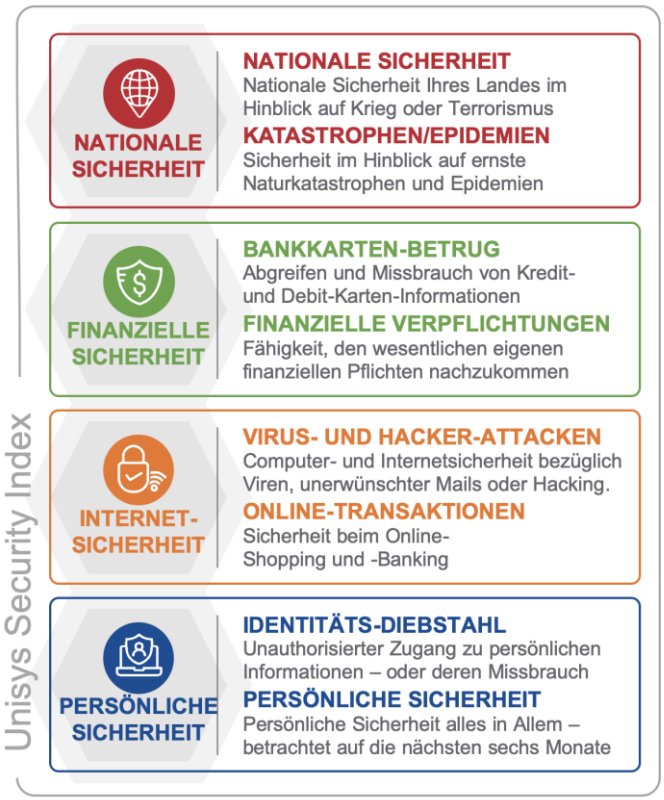
Unisys (NYSE: UIS) hat 2007 den Unisys Security Index eingeführt, einen jährlichen Überblick über Sicherheitsbedenken von Verbrauchern weltweit. Der Index ist ein errechneter Wert aus bis zu 300 Punkten, der die Einstellungen der Verbraucher in acht Sicherheitsbereichen aus vier Kategorien misst:

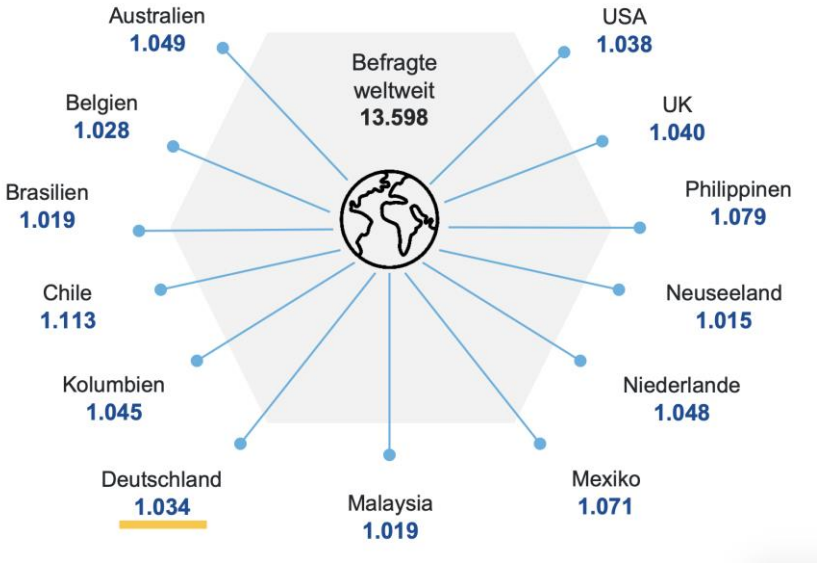
Der Unisys Security Index 2019 basiert auf nationalen Erhebungen repräsentativer Stichproben von 13.598 erwachsenen Bewohnern im Alter von 18 bis 64 Jahren. Die Interviews wurden in 13 Ländern online durchgeführt. Alle nationalen Umfragen wurden vom 27. Februar bis 22. März 2019 durchgeführt. Eine zusätzliche Frage zu Sicherheitsbedenken bei Großveranstaltungen wurde vom 3. April bis 12. April 2019 gestellt.

In allen Ländern wurde die Stichprobe nach nationalen demografischen Merkmalen wie Geschlecht, Alter und Region gewichtet.

Globale Sicherheitsindizes sind Durchschnittswerte der jeweiligen Sicherheitsindizes der 13 Länder. Die Fehlerquote beträgt +/- 3,1% pro Land bei einem Konfidenzniveau von 95% und +/- 0,9% für die globalen Ergebnisse.

Die Umfrage zum Unisys Security Index 2019 wurde von Reputation Leaders durchgeführt, einem globalen Beratungsunternehmen.

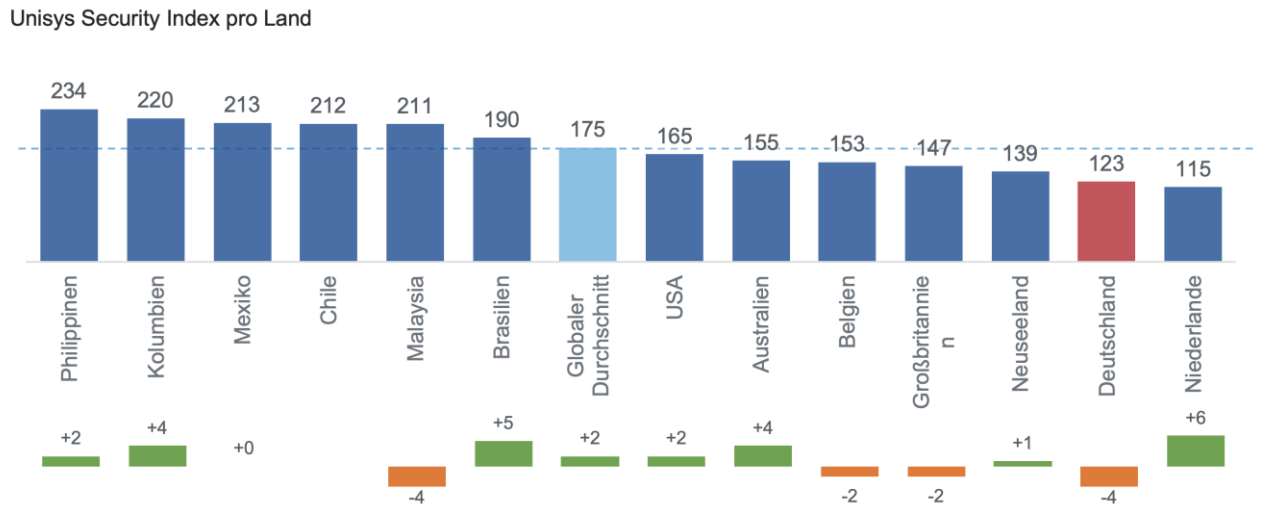




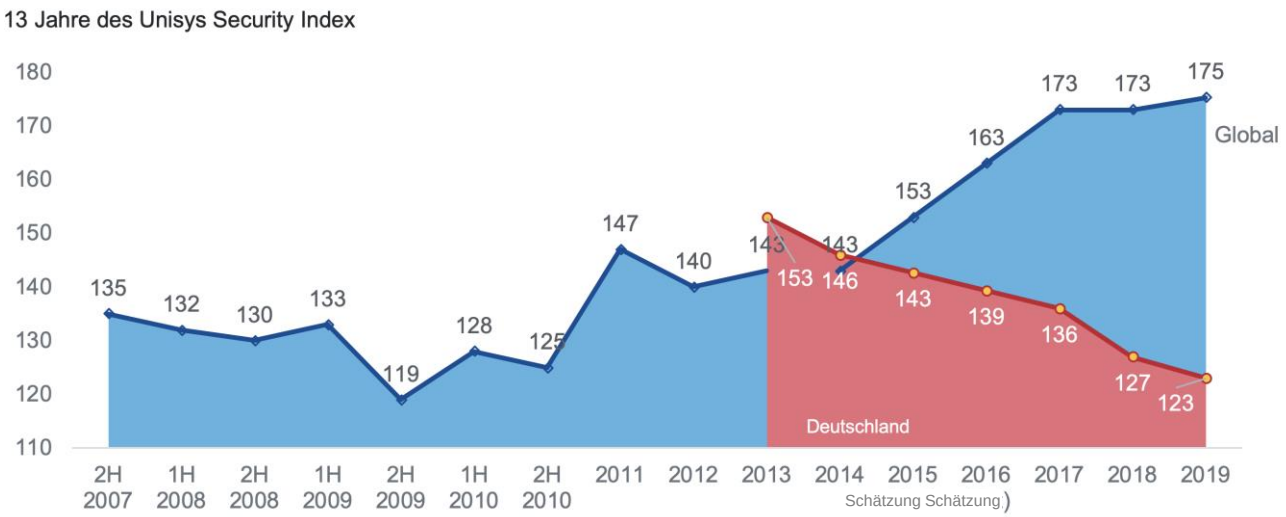
©2019 Unisys Corporation. Alle Rechte vorbehalten.

Sicherheitsbedenken in Deutschland

Der Unisys Security Index in Deutschland liegt 2019 bei 123 von maximal 300 Punkten und ist damit der zweitniedrigste weltweit. Nur in den Niederlanden liegt der Index noch niedriger (acht Punkte), dort nehmen die Sicherheitsbedenken jedoch zu.



Entgegen den weit verbreiteten Vorurteilen über eine typische „German Angst“ sind die Deutschen laut dem Unisys Security Index 2019 relativ unbesorgt. Während die globalen Sicherheitsbedenken seit 2007 in diesem Jahr am größten sind, sind die Sicherheitsbedenken der Deutschen das dritte Jahr in Folge zurückgegangen – und liegen nun auf einem historischen Tief von 123 Punkten.

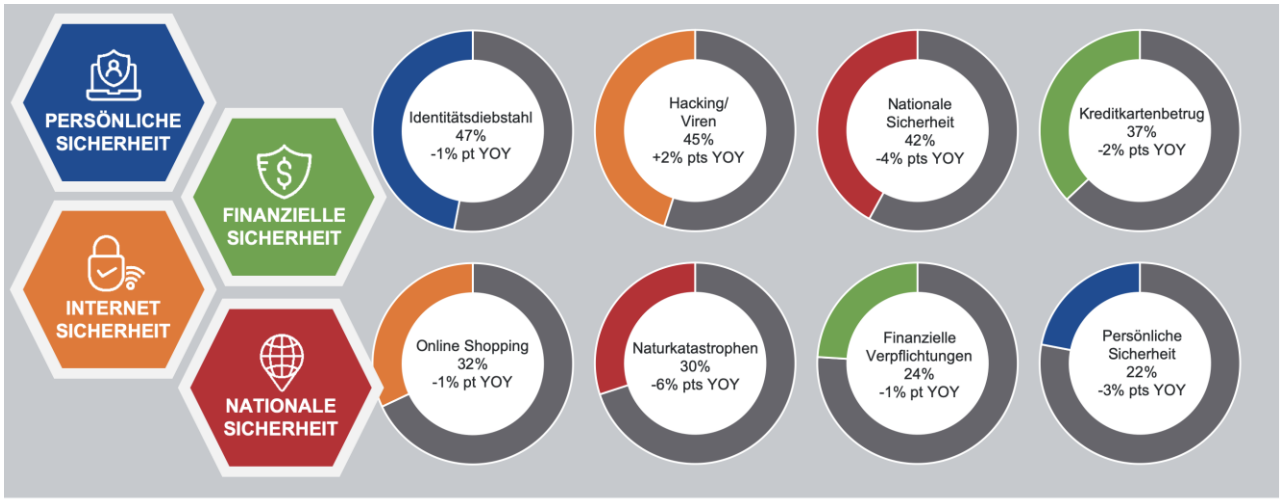


©2019 Unisys Corporation. Alle Rechte vorbehalten.

Sorge um die Internet-Sicherheit führt bei den Bedenken der Deutschen, während Ängste hinsichtlich der nationalen Sicherheit nachlassen.

Die Internet-Sicherheit ist in diesem Jahr – auch aufgrund eines deutlichen Rückgangs der Bedenken über nationale Sicherheit – zur dringendsten Sorge der Deutschen geworden.

Während die meisten Sorgen in Deutschland im vergangenen Jahr zurückgegangen sind, hat die Angst vor Viren und Hacking jedoch das dritte Jahr in Folge zugenommen. Dies spiegelt die globalen Trends wider, bei denen fast zwei Drittel der Verbraucher (63%) weltweit ernsthafte Bedenken hinsichtlich der Bedrohung durch Viren und Hacking angeben.



% pts=prozentpunkte

% ernsthaft besorgt (Wert aus „sehr“ und „extrem“ besorgt)
%=Prozentpunkte

©2019 Unisys Corporation. Alle Rechte vorbehalten.

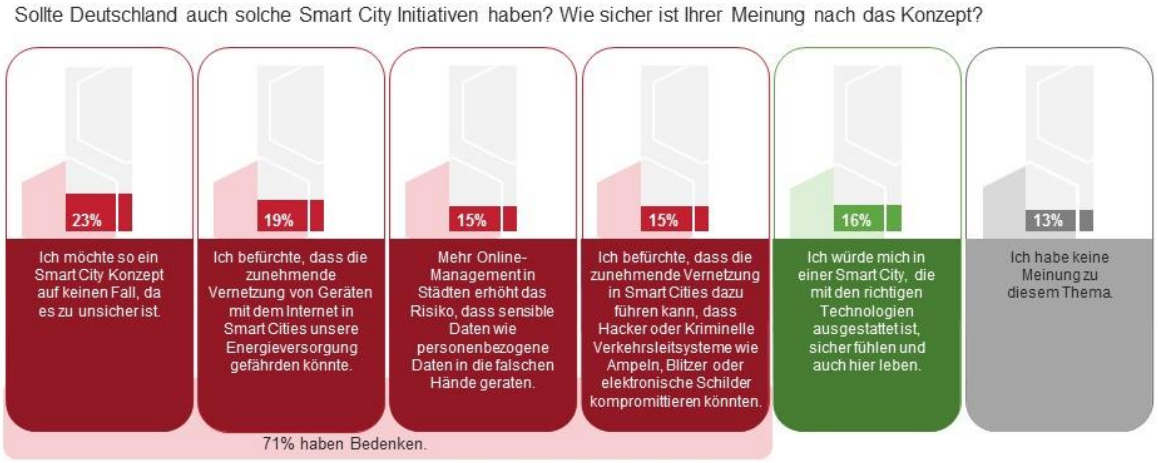
Zusätzliche Erkenntnisse für Deutschland

Im Rahmen des Unisys Security Index wird jedes Land zu bestimmten aktuellen Sicherheitsaspekten und -trends befragt. Im Jahr 2019 beantworteten die Deutschen unter anderem Fragen zu folgenden Themen:

- Smart-City-Initiativen und Bedenken der Deutschen über beteiligte Technologien, vor allem über privaten Gebrauch von Drohnen und autonomes Fahren.
- Einstellungen der Deutschen zum Einsatz von Video- und Bodycam-Überwachung im öffentlichen Raum.

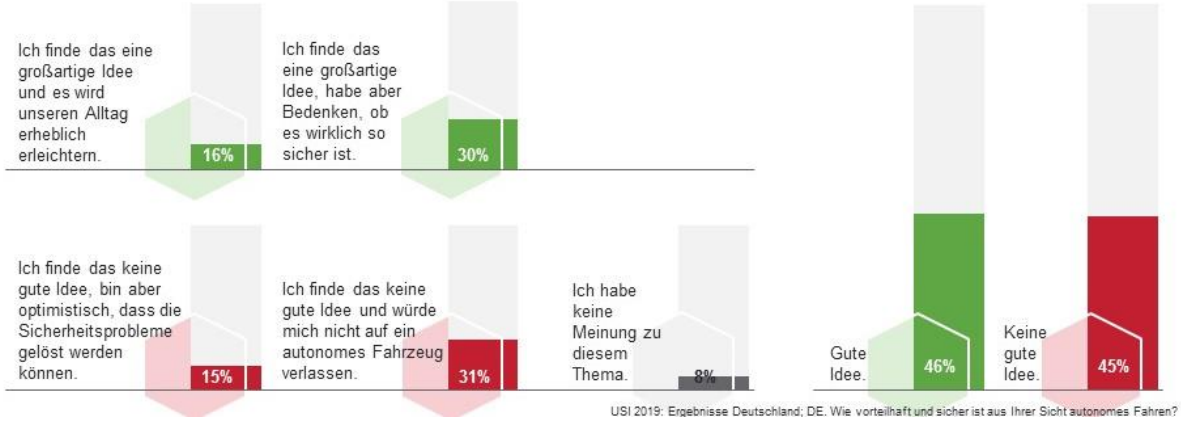
Deutsche sind ernsthaft besorgt über Smart City-Initiativen

Deutschland hat in den vergangenen fünf Jahren Milliarden von Dollar in Forschung und Technologie investiert und ist treibend in der Entwicklung von smarten Städten. Die Mehrheit der Deutschen hat zumindest ein gewisses Verständnis dafür, worum es bei solchen Konzepten geht. Fast drei Viertel (71%) der Deutschen sind jedoch ernsthaft besorgt über solche Initiativen und die damit verbundenen Technologien. Insbesondere haben die Deutschen Bedenken hinsichtlich der Sicherheit von Smart-City-Technologien. Sie fürchten etwa Risiken, die sich aus dem potenziellen Missbrauch sensibler Daten, aus der Bedrohung durch Hacker oder Kriminelle sowie aus möglichen Auswirkungen auf die Energieressourcen ergeben.



Autonomes Fahren und fahrerlose Autos sind aktuell Schwerpunktthemen in der Automobilindustrie. Deutschland ist diesbezüglich führend in Forschung und Entwicklung. In Bezug auf das autonome Fahren sind die Deutschen jedoch gespalten. Über 30% der im Unisys Security Index befragten Deutschen gaben an, kein Vertrauen in autonome Fahrzeuge zu setzen.

Wie nützlich und sicher ist autonomes Fahren in Ihren Augen?



Ich denke, das ist eine gute Idee, aber ich habe Bedenken, dass es nicht sicher ist. Drohnen werden ein wesentlicher Bestandteil bei der der Entwicklung von Smart Cities, doch die Herausforderungen in Bezug auf Sicherheit und Schutz der Privatsphäre sind ein großes Thema. Der Einsatz von Freizeit-

©2019 Unisys Corporation. Alle Rechte vorbehalten.

Drohnen erfreut sich wachsender Beliebtheit und ist in Deutschland relativ wenig keine Genehmigung zum Fliegen von Drohnen unter 5 kg erforderlich ist.

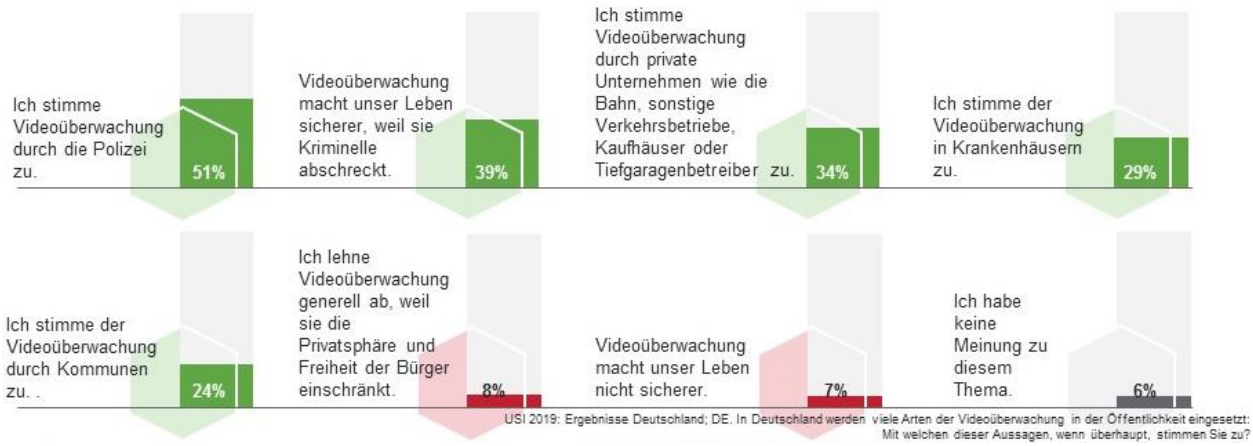
Mehr als 50% der im Unisys Security Index befragten Deutschen gaben an, dass sie nicht möchten, dass private Eigentümer Drohnen einsetzen. Dies ist vor allem auf Sicherheitsbedenken zurückzuführen, die durch den Einsatz von Drohnen in der Nähe von Flughäfen entstehen, sowie auf Bedenken hinsichtlich der Verletzung der eigenen Privatsphäre.

An öffentlichen Orten ist eine angemessene Überwachung erwünscht

Nach einer Reihe ernster Angriffe an öffentlichen Orten ergriff die Bundesregierung 2017 Maßnahmen zur Lockerung der Vorschriften für die Videoüberwachung.

Die Deutschen scheinen sich keine besonderen Sorgen über die Auswirkungen auf die Privatsphäre zu machen, und viele stimmen einer angemessenen Verwendung von Video- und Körperkamera-Überwachung an öffentlichen Orten zu. Über die Hälfte der Deutschen (51%) ist der Meinung, dass Videoüberwachung von der Polizei eingesetzt werden sollte, 39% sind der Meinung, dass Videoüberwachung das Leben sicherer macht, indem diese Kriminelle abschreckt. Und 34% sind der Meinung, dass private Unternehmen wie Transportunternehmen, Kaufhäuser und Parkhausbetreiber Videoüberwachung verwenden sollten.

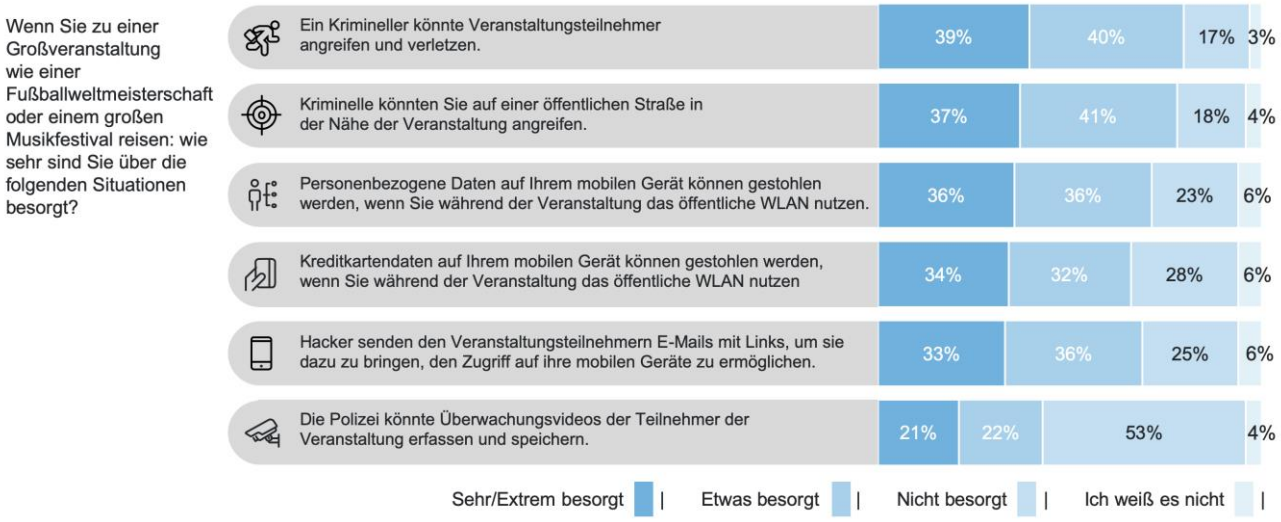
In Deutschland werden viele Formen der Video-Überwachung an öffentlichen Orten eingesetzt. Welcher der folgenden Aussagen würden sie zustimmen?



©2019 Unisys Corporation. Alle Rechte vorbehalten.

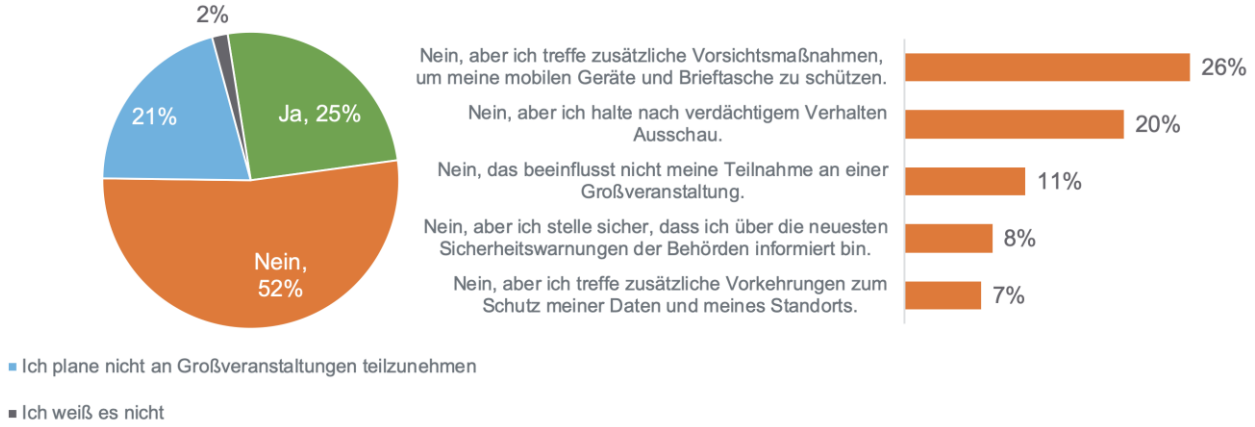
Sicherheitsbedenken bei Großveranstaltungen

In der ersten Jahreshälfte 2019 gab es massive Angriffe auf öffentliche Veranstaltungen auf der ganzen Welt, und die globalen Sicherheitsbedenken über die Teilnahme an Großveranstaltungen sind groß. Bei der Teilnahme an Großveranstaltungen sind die Deutschen unter anderem besorgt über die Gefahr von möglichen Körperverletzungen durch kriminelle Angriffe wie auch darüber, Opfer einer Cyberattacke zu werden.



Ein Viertel der Deutschen würde es sich aus Sicherheitsgründen zweimal überlegen, an großen Veranstaltungen teilzunehmen, und 16% haben ihre Pläne schon einmal geändert.

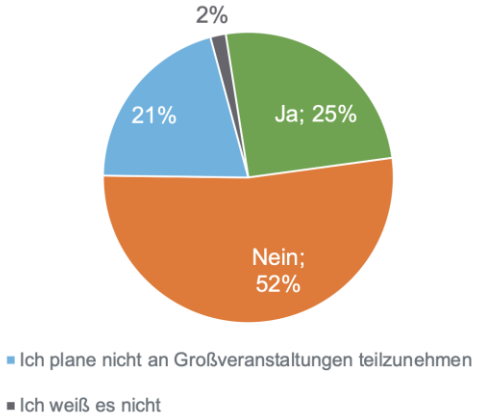
Hat die Tatsache, dass Ihre Daten gestohlen oder Sie ein Opfer von physischer Gewalt bei einer Großveranstaltung (wie einer Fußballweltmeisterschaft oder einem großen Musikfestival) werden können, dazu geführt, dass Sie zweimal über die Teilnahme an so einer nachgedacht haben?



©2019 Unisys Corporation. Alle Rechte vorbehalten.

Auch wenn 52% der Deutschen ihre Pläne für Großveranstaltungen noch nicht geändert haben, treffen doch 44% zusätzliche Sicherheitsvorkehrungen, z.B. zur Sicherung von mobilen Geräten und Brieftaschen – und achten verstärkt auf verdächtiges Verhalten.

Hat die Tatsache, dass Ihre Daten gestohlen oder Sie ein Opfer von physischer Gewalt bei einer Großveranstaltung (wie einer Fußballweltmeisterschaft oder einem großen Musikfestival) werden können, dazu geführt, dass Sie zweimal über die Teilnahme an so einer nachgedacht haben?



©2019 Unisys Corporation. Alle Rechte vorbehalten.

Die Unisys-Perspektive

Sicherheit bei Großveranstaltungen

Salvatore Sinno, Global Chief Security Architect bei Unisys, hat eine Liste einfacher Schritte zusammengestellt, die Menschen unternehmen können, um bei großen Sportveranstaltungen, Konzerten oder Festivals sicher zu bleiben:

1. **Kaufen Sie Veranstaltungstickets nur über offizielle Kanäle oder Websites, denen Sie vertrauen**. Stellen Sie sicher, dass auf der Website, auf der Sie Tickets kaufen, das sichere Schloss-Symbol im Browser angezeigt wird und die Adresse mit „https://" beginnt. Und wenn die Ticketpreise zu gut aussehen, um wahr zu sein, sollten Sie stutzig werden.
2. **Planen Sie im Voraus und überprüfen Sie die Warnungen der lokalen Behörden**. Melden Sie sich für alle Reise- oder Nachrichtenalarme an, die von den Veranstaltern bereitgestellt oder empfohlen werden, um über den Verkehr oder über Neuigkeiten zu möglichen Störungen am Veranstaltungstag informiert zu sein.
3. **Wenn Sie allein zu einer Massenveranstaltung gehen, lassen Sie es jemanden wissen**. Stellen Sie sicher, dass Ihre Freunde oder Ihre Familie wissen, wohin Sie gehen, wann Sie dort ankommen werden und wann Sie voraussichtlich wieder zurück sind.
4. **Reisen Sie mit leichtem Gepäck**. Es ist nicht nötig, alles, was man besitzt, auf ein Festival mitzunehmen. Lassen Sie die Wertsachen besser zu Hause und reisen Sie bescheiden – wenn möglich nur mit dem Nötigsten in der Tasche.
5. **Sobald Sie zur Veranstaltung kommen, erkunden Sie Ihre Umgebung**. Stellen Sie sicher, dass Sie wissen, wo die Ausgänge sind und vereinbaren Sie einen Treffpunkt mit Freunden, falls Sie sich von der Gruppe trennen sollten. Finden Sie heraus, wo Veranstaltungspersonal und Informationspunkte sind, damit Sie schnell mit jemandem sprechen können, wenn Sie ein Anliegen haben.
6. **Aktualisieren Sie Mobilgeräte und vermeiden Sie ungesicherte WLAN-Netze**. Stellen Sie sicher, dass Ihr Handy mit der neuesten Software aktualisiert ist, damit es so sicher wie möglich ist. Verwenden Sie nur passwortgeschütztes WLAN, denn ungeschützte Netzwerke können Hackern den Zugriff auf Ihre persönlichen Daten oder auf Finanzdaten erleichtern.
7. **Vermeiden Sie elektronische Transaktionen mit inoffiziellen Stellen**. Seien Sie auch besonders vorsichtig mit kontaktlosen Zahlungen oder mobilen Transaktionen, denn hier könnten Datensammler relativ leichtes Spiel haben, Ihre Finanzdaten abzugreifen – um sie zu selbst verwenden oder weiter zu verkaufen.
8. **Achten Sie auf verdächtiges Verhalten bei Großveranstaltungen**. Scheuen Sie sich nicht, etwas, das Sie für ungewöhnlich halten, auch zu melden – wie etwa unbeaufsichtigtes Gepäck oder Menschen, die sich verdächtig oder bedrohlich verhalten.
9. **Halten Sie Ihr Mobiltelefon für Notfälle aufgeladen**. Wenn möglich, nehmen Sie ein Akkuladegerät mit, um sicherzustellen, dass Ihr Handy immer verfügbar ist, wenn Sie es brauchen.
10. **Bleiben Sie im Notfall ruhig und bewegen Sie sich an den Rand von Menschenmassen**. Versuchen Sie, das Risiko-Gebiet zügig und ruhig zu verlassen. Wenn Sie müssen, treten Sie eine rasche Flucht an, verstecken Sie sich bei Bedarf, rufen Sie den Notruf an, wenn Sie können, und lassen Sie dann Ihre Familie wissen, dass Sie sicher sind.

©2019 Unisys Corporation. Alle Rechte vorbehalten.

DIE SORGE DER VERBRAUCHER WÄCHST

Angesichts der politischen Turbulenzen der letzten Jahre, kombiniert mit Berichten über Vorfälle von körperlicher Gewalt und einer scheinbar endlosen Reihe von Cyberangriffen auf Regierungen und Privatunternehmen, ist es nicht verwunderlich, dass der Unisys Security Index in den Jahren, in denen die Umfrage durchgeführt wurde, in diesem Jahr das höchste Maß an globalen Sicherheitsbedenken bei Einzelpersonen verzeichnete. „Es gibt Sicherheitsbedenken an jedem Ort der Welt, in jeder Branche, bei allem, was Sie tun – und zwar in massivem Umfang“, so Chris Kloes, Vice President von Unisys Security Solutions.

Das anhaltende Wachstum der Besorgnis kann zumindest teilweise auf ein stärkeres Bewusstsein der Verbraucher für Bedrohungen zurückzuführen sein, die sowohl in der Online- als auch in der Offline-Welt bestehen. Dieses wachsende Bewusstsein hat auch dazu geführt, dass die Verbraucher Unternehmen durchaus kritisch sehen, die mit ihren personenbezogenen Daten umgehen. „Die Gesellschaft beginnt aufzuwachen und zu erkennen: Persönliche Daten sind absolut wichtig – und gelangen sie in die falschen Hände, können Menschen damit ernsthaften Schaden anrichten“, so Jeff Livingstone, Unisys Vice President und Global Head of Life Sciences & Healthcare.

„Im Gesundheitswesen nehmen die allgemeinen Bedenken in Bezug auf die Sicherheit personenbezogener Daten und bezüglich der Privatsphäre rasant zu", so Livingstone weiter. „Gründe können unter anderem bekannt gewordene Datenlecks der vergangenen Jahre sowie ausufernde Hackerangriffe sein.“

Als weiterer Faktor kommt hinzu, dass gerade im Gesundheitswesen Leistungs- und Abrechnungsprozesse zeitlich oft relativ weit voneinander entfernt sind. Dies gibt Hackern teilweise viel Raum, um in laufende Prozesse einzudringen und dort Schaden anzurichten. Attraktiv sind diese Daten für Hecker vor allem, da Gesundheits-Informationen sich gut dazu eignen, um online ganze Persönlichkeits-Profile anzulegen. Daher sind diese Daten für Cyberkriminelle oft noch wertvoller als „nur“ klassische Finanzinformationen. Der Wert von Gesundheits-Informationen auf dem Schwarzmarkt nimmt aus diesem Grund derzeit auch exponentiell zu. All diese Aspekte bilden eine ernst Bedrohungskulisse, die direkt die Verbraucher ins Visier nimmt.

Maria Allen, Vice President und Global Head of Financial Services bei Unisys, weist auf einen ähnlichen Trend bei Finanzinstituten hin. „Es gibt immer mehr digitale Informationen, und die Banken sind interessiert an digitalen Lösungen und Automatisierung. Dies führt auch bei Verbrauchern zu neuen Fragen und zu konkreten Bedenken bei vielen Aspekten des Sicherheitsempfindens."

Interessanterweise werde dieser Trend z.B. durch Projekte von Gesundheitsdienstleistern, den Service für die Kunden durch Technologie zu verbessern, teils noch verschärft, so Kloes. „Viele Unternehmen nutzen heute Technologien, um dem Verbraucher mit neuen Apps und Geräten mehr Möglichkeiten und Wahlfreiheit zu geben“, betont er. „Das kann jedoch Risiken bergen, wenn etwa weder Verbraucher noch die Dienstleister selbst wirklich auf die neuen Angebote vorbereitet sind. Der Verbraucher wird natürlich annehmen, dass Apps auf seinem Handy sorgfältig geprüft und sicher sind; doch immer wieder tun sich Lücken auf zwischen der Wahrnehmung der Endanwender und der Fähigkeit der Dienstleister, wirklich alle Aspekte der Cybersicherheit zu berücksichtigen und zu bedienen.“

SICHERHEITSBEDENKEN ERSTRECKEN SICH AUCH AUF FREIZEITAKTIVITÄTEN WIE DIE TEILNAHME AN GROSSVERANSTALTUNGEN.

Regierungen und private Organisationen konzentrieren sich seit langem auf die Gewährleistung der physischen Sicherheit, wenn es um die Teilnehmer an Veranstaltungen wie etwa Olympischen Spielen oder Weltmeisterschaften geht. In den vergangenen Jahren haben jedoch mehrere massive Tragödien bei Konzerten und anderen großen Veranstaltungen Anlass zur Sorge im Zusammenhang mit entsprechenden Events gegeben – ob auf lokaler, nationaler oder internationaler Ebene. Die Ergebnisse des Unisys Security Index 2019 zeigen in diesem Zusammenhang übrigens, dass sich die Verbraucher bei öffentlichen Veranstaltungen ebenso um die Sicherheit ihrer Daten sorgen wie um ihre physische Sicherheit.

©2019 Unisys Corporation. Alle Rechte vorbehalten.

Dies wirft die Frage auf, wie staatliche Sicherheitsbehörden, Veranstaltungsorganisatoren und andere Beteiligte das breite Spektrum an geäußerten Bedenken angehen können.

Mark Forman, Unisys Vice President und Global Head of Public Sector, betont, dass einige Regierungen und Unternehmen bereits Wege finden, um physischen Schutz und Cybersicherheit zusammenzubringen. „In den USA wurden beispielsweise Fusionszentren eingerichtet, um eine bewusste Zusammenarbeit zu fördern, die sowohl für die Cybersicherheit als auch für die physische Sicherheit nützlich ist. Es gibt US-Bundesstaaten, die hier bereits führend sind, weil sie über sehr guten Informationsaustausch verfügen. Dazu gehören moderne Technologien und Menschen, die bereit sind, Informationen auszutauschen sowie mit Informationen – auch aus externen Quellen – zu arbeiten. Und diese bestmöglich zu nutzen: natürlich innerhalb der operativen, strategischen und gesetzlichen Richtlinien. Dies erfordert eine vertrauensvolle und sichere Zusammenarbeit aller Beteiligten."

IDENTITÄTSDIEBSTAHL WIRD WEITERHIN ALS GROSSE BEDROHUNG BETRACHTET

Mathew Newfield, Chief Information Security Officer von Unisys, stellt fest, dass sich die wachsende Bedeutung von Online-Identitäten für Verbraucher inzwischen auf fast jeden Aspekt des Lebens erstreckt. „Aus meiner Sicht stellt Identitätsdiebstahl einen bedeutenden Teil der Sicherheits-Diskussion dar", so Newfield. „Es gibt ein wachsendes Bewusstsein in der Welt, dass der Diebstahl der digitalen Identität Bankkarten, Finanzen, Steuererklärungen, Online-Shopping und noch vieles mehr massiv gefährden kann. Die Menschen erfahren langsam, dass man Identitäten in großem Umfang für weniger als einen Dollar pro Stück kaufen kann – und das macht den Leuten Angst."

Newfield fügt hinzu, dass die Folgen von Identitätsdiebstahl von Land zu Land unterschiedlich sein können: „In den USA und einigen anderen modernen Ländern gibt es z.B. Schutzmechanismen, die in der Regel greifen, sobald Bankdaten gestohlen und missbraucht werden", erläutert er. „Wenn ich dadurch auf der Bank liegendes Geld verliere, bin ich weitgehend geschützt. Aber das gilt nicht für jedes Land – und so kann es herbe und einschneidende Konsequenzen von Identitätsdiebstahl für viele Menschen in verschiedenen Regionen der Welt geben."

Laut Allen hat das global wachsende Unbehagen der Verbraucher jedoch auch sein Gutes, da so die Aufmerksamkeit für Bedrohungen steige und Verbraucher alles in Allem wachsamer und in Sicherheitsfragen anspruchsvoller werden könnten. Auch mit Blick auf Organisationen, mit denen sie zu tun haben, und von denen sie sich wünschen, ihre Identität zu schützen. „Identitätsdiebstahl ist ein enormes Thema", betont sie. „Und es ist an der Zeit, dass auch ganz normale Verbraucher auf der ganzen Welt das erkennen. Ich freue mich, dass dies aus der Umfrage hervorgeht."

WACHSENDE BESORGNIS KANN DURCH MEDIEN UND POLITIK BEEINFLUSST WERDEN.

Forman erklärt, dass der Unisys Security Index die Wahrnehmung der Verbraucher in Sicherheitsfragen misst. Da diese jedoch teils von Faktoren wie Medien und Politik beeinflusst würde, sei die ge-äußerte Wahrnehmung nicht immer völlig mit der Realität gleichzusetzen.

„Wenn man sich die Teile der Welt ansieht, in denen es erhöhte Werte gibt, insbesondere im Bereich der persönlichen Sicherheit, dann finden sich dort oft nationalistische Bewegungen, und die Politik hat Sicherheitsfragen besonders hervorgehoben", erläutert er. „Wahrnehmung basiert immer auch auf dem, was in den Medien berichtet wird, und kann Bedenken fördern. So liegt es nahe, dass es einen gewissen Zusammenhang zwischen einem höheren Besorgnisniveau und nationalistischen Bewegungen gibt. Die Frage ist natürlich: Ist die nationalistische Bewegung das Ergebnis tatsächlicher Risiken – oder sind die Zahlen das Ergebnis nationalistischer Politik, die Ängste schürt?"

©2019 Unisys Corporation. Alle Rechte vorbehalten.

Fazit

Verbraucher-Bedenken wachsen im Durchschnitt weltweit – in allen Bereichen der Sicherheit und über die meisten Bevölkerungsschichten hinweg. Diese Bedenken sind durchaus bedeutend für Unternehmen und öffentliche Einrichtungen, da sich Verbraucher darauf verlassen möchten, dass hier ihre Daten sicher sind und geschützt werden. Diese Organisationen müssen der Sicherheit daher absolute Priorität einräumen, um nicht selbst Bedenken zu fördern. Ein konsequenter Zero-Trust-Ansatz kann dabei helfen, alle im Unternehmen tätigen Akteure, Systeme und Dienste zu identifizieren und abzusichern.

Was jetzt zu tun ist

Was können Unternehmen und Regierungsbehörden, die mit Verbrauchern und Bürgern zu tun haben, also konkret verbessern? Unisys empfiehlt:

1. *Machen Sie sich auf den Weg zu einem Zero-Trust-Sicherheitskonzept, das Ihren gesamten Netzwerkverkehr ins Visier nimmt*

Die zunehmende Besorgnis der Verbraucher über die Online-Sicherheit, die sich im Unisys Security Index 2019 widerspiegelt, unterstreicht die anhaltende Notwendigkeit, alle möglichen Maßnahmen zu ergreifen, um modernsten Datenschutz für Kunden zu gewährleisten, wenn sie mit einer Organisation zusammenarbeiten.

Unisys empfiehlt eine fünfstufige Methodik als Fahrplan, um zu einer vollständigen Zero-Trust-Implementierung zu gelangen. Die fünf Schritte zum Zero-Trust-Modell sind:

- Priorisieren: Der Zero-Trust-Weg beginnt mit einer vollständigen Transparenz des Ökosystems, was es Unternehmen ermöglicht, Schwachstellen zu verstehen und Prioritäten zu setzen.
- Schützen: Basierend auf den Prioritäten müssen Unternehmen zunächst ihre am stärksten gefährdeten Menschen, Geräte und Netzwerke schützen – und dann den Schutz auf alle ausdehnen.
- Vorhersage: Unternehmen müssen Bedrohungen vorausschauend begegnen und ihre Risikohaltung durch KI-gestützte prädiktive Gefahrenabwehr sowie durch objektive, datengesteuerte Cyber-Risikoprognosen stärken.
- Isolieren: Unternehmen sollten kritische Daten und Systeme isolieren und so den potenziellen Zugriff von unerwünschten Benutzern verhindern.
- Beheben: Unisys hilft Unternehmen, die operativen Auswirkungen von Angriffen zu minimieren, indem es die Reaktionszeit bei möglichen Vorfällen minimiert.

„Unisys Security Solutions sorgt für die Implementierung einer Zero-Trust-Architektur, die mit Unternehmen mitwächst“, so Kloes. „Unisys nutzt dynamische Isolation, um Geräte oder Benutzer beim ersten Anzeichen von Kompromittierung zu isolieren – und identifiziert, bewertet und sichert vertrauenswürdige Benutzer, Geräte und Datenflüsse.“

2. *Moderne Sicherheits-Technologie und menschliches Verständnis*

Zeitgemäße Sicherheitstechnologie kann einen wichtigen Beitrag zur Analyse von Netzwerkaktivitäten und zur Identifizierung von Sicherheitsproblemen leisten, bevor diese eskalieren. Aber auch die beste Technologie wird nicht wirklich effektiv sein, ohne verständige Menschen, die Daten und Analyse-ergebnisse verstehen, sie interpretieren und danach handeln können. Unisys empfiehlt Unternehmen daher, stets auf neueste Technologie zu setzen – und dabei immer auch die Menschen mitzunehmen und zu begeistern, damit Kundenerwartungen optimal adressiert werden.

„Sicherheit ist eine mehrdimensionale Disziplin", so Forman. "Die Technologie kann viel für die Zusammenstellung und Analyse von Informationen tun – aber es braucht auch die richtigen Leute, um gewonnene Erkenntnisse zielorientiert zu nutzen. Wir sehen dies beispielsweise bei der Grenzsicherheits-Technologie, die sich oft auf Datenanalyse konzentriert: Digitale Informationen zu erheben und zu sammeln, ist hier das eine. Aber verwertbare Einsichten aus den Daten zu generieren sowie auf der Grundlage von Daten zu kommunizieren und zu entscheiden, ist das andere, um wirklich effektiv auf Datenbasis zu arbeiten."

©2019 Unisys Corporation. Alle Rechte vorbehalten.

3. *Risikobewältigung angesichts einer wachsenden Zahl von Devices*

Die Ergebnisse des Unisys Security Index 2019 verdeutlichen, dass die Grenze zwischen physischer Sicherheit und Online-Sicherheit in der Wahrnehmung vieler Menschen verschwimmt. Bedenkenswert ist zudem, dass es in den meisten Organisationen immer mehr mobile Geräte gibt, die an physisch riskante Orte mitgenommen werden können, wo unter Umständen Verlust oder Diebstahl drohen.

> Während außerdem viele Unternehmen hart daran arbeiten, die physische Sicherheit ihrer Mitarbeiter zu gewährleisten und zu verbessern, erhält die Sicherheit der Daten möglicherweise nicht immer so viel Aufmerksamkeit, wie es wünschenswert ist.
>
> Müssen sich Mitarbeiter an vergleichsweise riskanten Orten außerhalb des Unternehmens aufhalten, tun Unternehmen zudem gut daran, Möglichkeiten zur Datensicherung unterwegs zur Verfügung zu stellen und Praxis-Hinweise zu geben, wie sich Risiken minimieren lassen.
>
> *„Viele Unternehmen denken nicht daran, ihre Mitarbeiter und Führungskräfte auch bei der physischen Sicherheit außerhalb der eigenen Organisation zu unterstützen – etwa, wenn sie an vergleichsweise riskante Orte reisen“, so Livingstone. „Unternehmen sollten daher die Geräte und Daten dieser Mitarbeiter schützen und ihren Leuten zudem konkrete Hilfestellungen geben, die etwa Unterkunft, Aufenthaltsorte oder Mobilität am Zielort betreffen.“*

4. *Identitäts-Absicherung durch Biometrie und Co.*

Die eigene, eindeutige Identität öffnet Türen: für Online-Transaktionen, für den persönlichen, physischen Zugang zu sicherheitsrelevanten Einrichtungen (etwa an Flughäfen) oder an Grenzen zu anderen Ländern. Regierungsorganisationen und Unternehmen können ihren Bürgern und Kunden das Leben deutlich leichter machen, wenn sie Sicherheitsstandards gewährleisten, die technologisch modernsten Ansprüchen genügen, die eindeutig, manipulationssicher und günstig sind – und dabei einfach und anwenderfreundlich.

> *„Unsere eigenen Identitäten sind mit das Kritischste, was wir im Leben haben", so Vishal Gupta, Senior Vice President und Chief Technology Officer bei Unisys. „Der Unisys Security Index zeigt deutlich, dass die Menschen bereit sind, Biometrie zu verwenden, um sie physisch und online zu schützen. Leider zeigt die Umfrage auch, dass viele Verbraucher Unternehmen und Organisationen nicht zutrauen, ihre biometrischen Daten angemessen zu schützen. Unternehmen und Behörden müssen daher konkrete Maßnahmen ergreifen, um die persönlichen Daten ihrer Kunden zu schützen. Sinnvoll ist, Produkte wie Unisys Stealth® einzusetzen, um die kritischsten Daten zu isolieren und sie vor Eindringlingen zu schützen, die immer wieder Wege in digitale Umgebungen suchen werden."*

Weitere Informationen über die Sicherheitsangebote von Unisys finden Sie unter: www.unisys.com/security.

©2019 Unisys Corporation. Alle Rechte vorbehalten.

Über Unisys

Unisys ist ein globales IT-Unternehmen, das leistungsfähige und sicherheitszentrierte Lösungen für die Unternehmen und Regierungsorganisationen weltweit entwickelt. Das Angebot von Unisys umfasst Sicherheitssoftware und -services, digitale Transformationsprozesse, Dienstleistungen rund um den modernen Arbeitsplatz, Industrieanwendungen und -services sowie innovative Softwareumgebungen für Enterprise-Anwendungen. Weitere Informationen darüber, welche Vorteile Unisys seinen Kunden aus dem öffentlichen Sektor sowie den Bereichen Finanzdienstleistungen und Handel bietet, finden Sie unter www.unisys.com.

Über den Unisys Security Index

Unisys führt seit 2007 den Unisys Security Index durch – die am längsten dauerhaft durchgeführte Momentaufnahme globaler Sicherheitsbedenken von Verbrauchern. Der Index ist ein berechneter Score aus 300 Punkten, der die sich im Laufe der Zeit ändernden Einstellungen der Verbraucher in acht Sicherheitsbereichen in vier Kategorien umfasst: nationale Sicherheit und Katastrophen/Epidemien in der Kategorie nationale Sicherheit; Bankkartenbetrug und finanzielle Verpflichtungen in der Kategorie finanzielle Sicherheit; Viren/Hacker und Online-Transaktionen in der Kategorie Internet-Sicherheit; Identitätsdiebstahl und persönliche Sicherheit in der Kategorie persönliche Sicherheit. Der Unisys Security Index 2019 basiert auf Online-Umfragen, die vom 27. Februar bis 22. März 2019 unter national repräsentativen Stichproben von mindestens 1.000 Erwachsenen in jedem der folgenden Länder durchgeführt wurden: Australien, Belgien, Brasilien, Chile, Kolumbien, Deutschland, Malaysia, Mexiko, Niederlande, Neuseeland, Philippinen, Großbritannien und die USA. Die Fehlerquote auf Länderebene beträgt +/-3,1% bei 95% Konfidenzniveau und +/-0,9% auf globaler Ebene.

Weitere Informationen zum Unisys Security Index 2019 finden Sie unter www.unisyssecurityindex.com.

©2019 Unisys Corporation. Alle Rechte vorbehalten.