DELL Technologies

Endpoint Security als wesentlicher Bestandteil von Zero Trust

Drei Empfehlungen zur Umsetzung von Zero Trust

DELL Technologies

Zusammenfassung

Zero Trust ist ein langfristiges Vorhaben. Es ist nicht ein Produkt oder eine Lösung, das bzw. die Unternehmen einfach so implementieren können. Es ist ein strategisches Framework für das Sicherheitsmanagement, das im Laufe der Zeit aufgebaut wird. Dieses E-Book enthält praktische Tipps für IT-EntscheidungsträgerInnen, die eine Zero-Trust-Transformation vornehmen. Der Fokus liegt dabei speziell darauf, welche Rolle die Sicherheit von Endpunkten bei der Schaffung einer modernen und wirklich sicheren Basis für das ortsunabhängige Arbeiten spielt.

Inhaltsverzeichnis

Die Cyber-sicherheits-lage

In der Arbeitswelt von heute spielen mobiles Arbeiten sowie Hybrid- und Cloud-Modelle eine immer größere Rolle, wodurch auch Sicherheitsbedrohungen zunehmen.

Der Schutz von Datenbeständen in Unternehmen ist in den letzten Jahren wesentlich komplexer geworden. Die Cloud hat sich als bahnbrechende Technologie für die Unternehmensproduktivität erwiesen und das mobile Arbeiten bzw. die Hybridarbeit nimmt beständig zu. Doch das hat auch seinen Preis. Der Umstieg vom Management reiner Vor-Ort-Infrastruktur zur Einbeziehung der Cloud hat die Angriffsfläche für böswillige Akteure vergrößert – und die Folgen sind weitreichend. Ein erfolgreicher Angreifer kann beispielsweise nicht nur einen Kunden, sondern womöglich sämtliche Kunden des betreffenden Cloud-Service und auch wiederum deren Kunden beeinträchtigen, also die gesamte Lieferkette. Dies kann für Bedrohungsakteure, die sowohl staatlicher Natur sein können als auch gewöhnliche Kriminelle, überaus lohnenswert sein. Aus diesem Grund werden sie immer neue Sicherheitslücken suchen, die sie ausnutzen können.

Die Cyberkriminalität soll Prognosen zufolge **bis 2025** weltweit Schäden in Höhe von **10,5 Bio. US-Dollar** verursachen.[i]

In einer Studie aus dem Jahr 2022 berichtet Verizon von **5.200** bestätigten Datenschutz-verletzungen. Das sind **1,3-mal mehr als im Vorjahr.**[ii]

Die Folgen für die vom ortsunabhängigen Arbeiten geprägte Welt

Unternehmen müssen eine Möglichkeit finden, sich für die sich entwickelnde Bedrohungslandschaft zu wappnen.

Was sind also die Folgen des zunehmenden Trends mobiler Arbeit? Im Wesentlichen gibt es hier zwei wichtige Punkte:

Alle Unternehmen sind angreifbar …

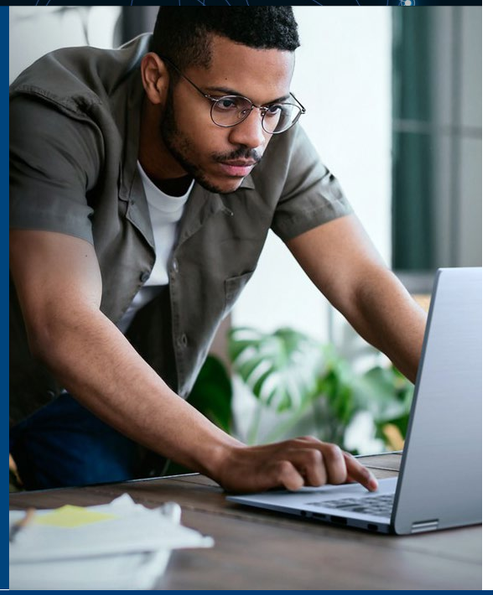
> „[W]enn ein zielstrebiger Akteur in Ihr System gelangen möchte, ist es sehr wahrscheinlich, dass ihm dies auch gelingt."
>
> – *Admiral Michael Rogers, ehemalige Führungskraft bei der National Security Agency und ehemaliger Kommandeur der U.S. Cyber Command*[iii]

… und bei Versagen können die Kosten existenzgefährdend sein.

> „2022 haben die Kosten einer Datenschutzverletzung mit durchschnittlich 4,35 Mio. US-Dollar einen neuen Höchststand erreicht [12,7 % mehr als noch 2020]."[iv]

Die Angriffsvektoren nehmen zu, die Angriffsfläche vergrößert sich und kein Unternehmen kann jemals vollkommen sicher sein. Unternehmen müssen vom Worst Case ausgehen und ihre Abwehr für den unvermeidlichen Angriff auf Vordermann bringen.

69 % der Unternehmen haben wegen einer schlecht gemanagten Internetressource eine Form von Cyberangriff erlebt.[v]



Warum sich Sicherheits-strategien ändern müssen

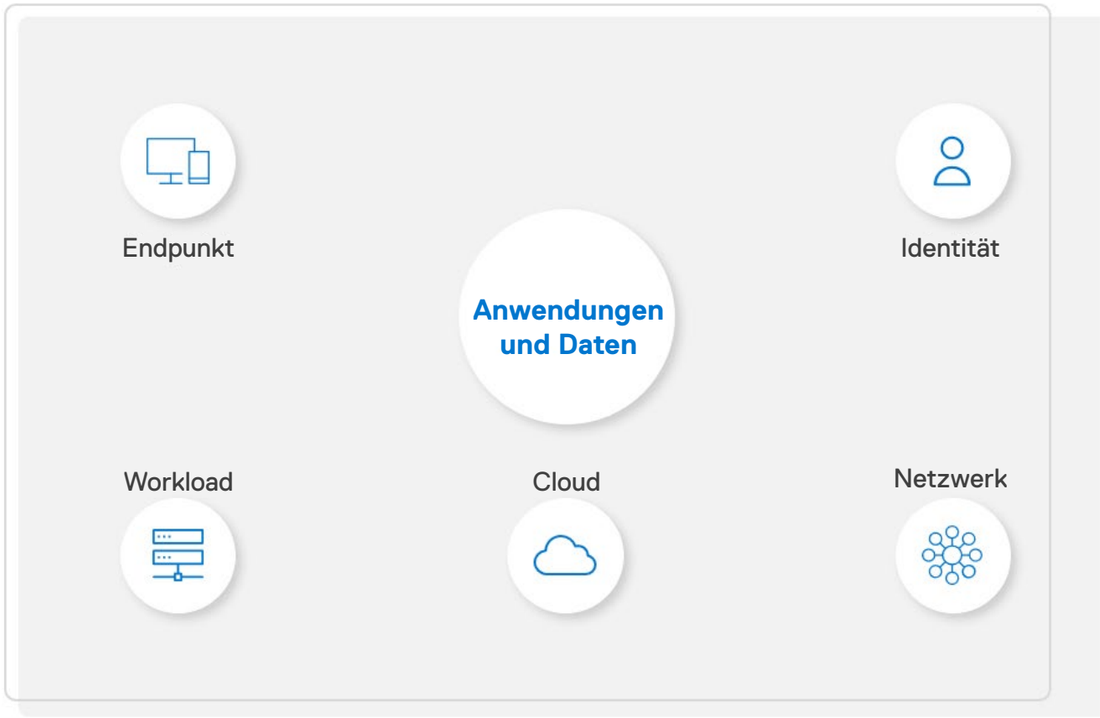
Wir müssen Cloud-basierte Umgebungen bestmöglich nutzen. Hier kommt Zero Trust ins Spiel.

Die klassischen Sicherheitsmodelle funktionieren nicht mehr. Und dafür gibt es gute Gründe.

Für einen effektiven Sicherheitsstatus müssen Unternehmen fünf Kontrollpunkte berücksichtigen: Endpunkt, Workload, Identität, Netzwerk und Cloud. Das Ziel ist, die Anwendungen und die Daten zu schützen.

Herkömmliche Ansätze sind oft isoliert, weshalb Unternehmen, die sie nutzen, auch anfälliger für Angriffe sind.

Weiter ...

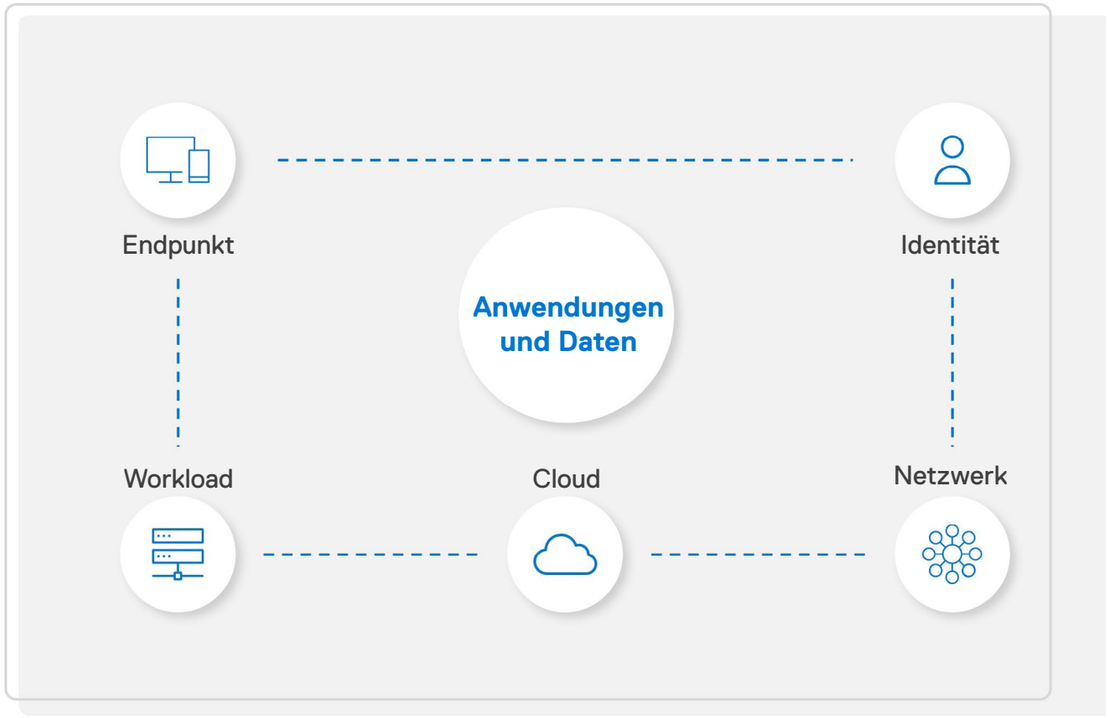


Warum sich Sicherheits-strategien ändern müssen

Wir müssen Cloud-basierte Umgebungen bestmöglich nutzen. Hier kommt Zero Trust ins Spiel.

Moderne Ansätze sind auf mehr Kontrolle ausgerichtet, mit besserer Kommunikation zwischen den Kontrollpunkten. Doch wenn wir verstärkt auf eine mobile oder Hybrid-Arbeitsumgebung setzen, müssen wir auch den Perimeter weiter stärken.

Weiter ...

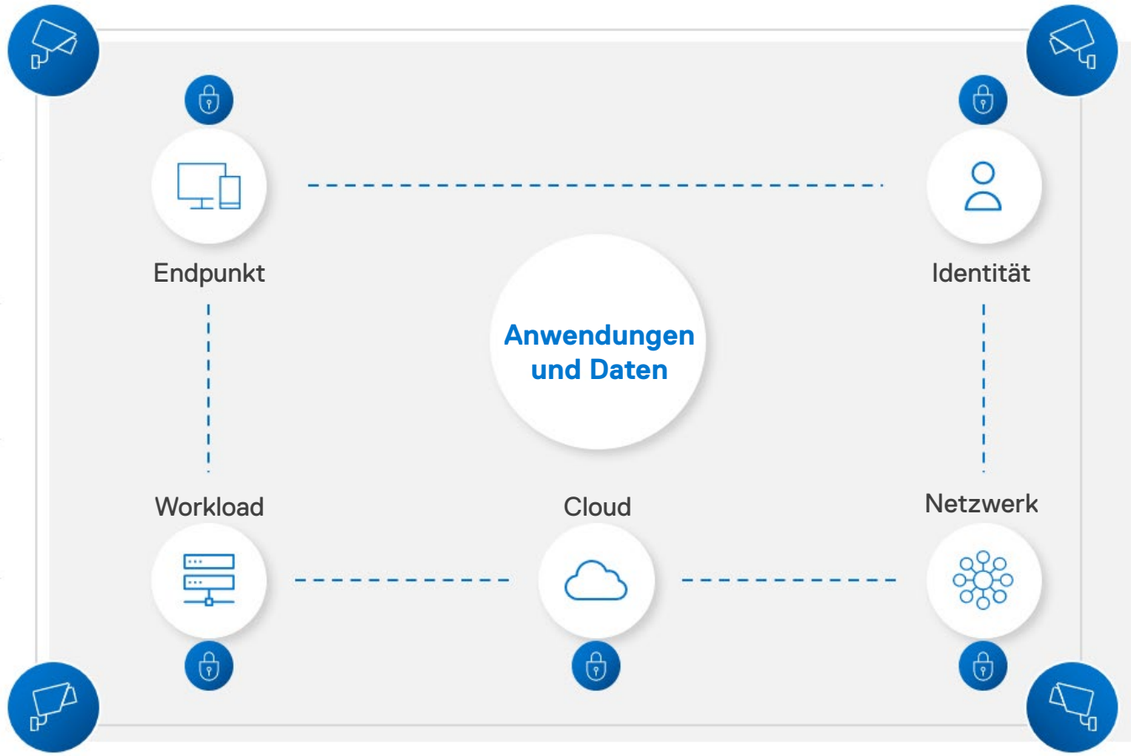


Warum sich Sicherheits-strategien ändern müssen

Wir müssen Cloud-basierte Umgebungen bestmöglich nutzen. Hier kommt Zero Trust ins Spiel.

MitarbeiterInnen arbeiten heute von überall aus – zu Hause, in Cafés, in Hotels – und verwenden dabei oft ungesicherte Wi-Fi-Netzwerke mit beschränkter bis keiner Konnektivität zu den durch Firewalls geschützten Büros oder Rechen-zentren. Standardmäßig wird womöglich eine direkte Verbindung von ihren Geräten zum Internet hergestellt, von wo aus die MitarbeiterInnen Cloud-Dateiserver und SaaS-Anwendungen (Software as a Service) nutzen – und mit Unternehmensdaten arbeiten.

In Anbetracht der immer ausgeklügelteren Angriffe und zunehmenden Anzahl an Angriffsvektoren funktionieren auf implizitem Vertrauen basierende Sicherheitsstrategien nicht mehr. Hier kommt Zero Trust ins Spiel.

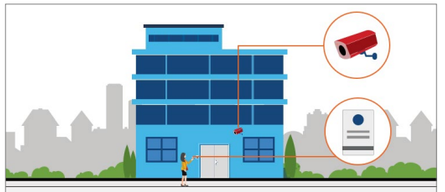


Die Grundlagen von Zero Trust

Zero Trust ist eine neue Herangehensweise an das Thema Sicherheit. Es ersetzt das *implizite* Vertrauen, was bedeutete, dass NutzerInnen nach der Authentifizierung im Netzwerk frei handeln können. Zero Trust leitet einen Paradigmenwechsel ein und gibt Unternehmen die explizite Kontrolle über ihre IT-Umgebung.

Wir können Zero Trust mit einem bekannten Konzept verdeutlichen: Sicherheitsprotokollen in Gebäuden.

Sie arbeiten bei einem Unternehmen im Büro. Bei Ihrer Einstellung haben Sie einen Mitarbeiterausweis erhalten und die Sicherheitsprotokolle gelernt. Sie betreten jeden Tag das Gebäude. Überall gibt es Kameras. Sie zeigen Ihren Mitarbeiterausweis an mehreren Stellen vor. An Ihrem Schreibtisch entsperren Sie dann Ihren Computer mit einem Kennwort.



Eine Mitarbeiterin kommt am Bürogebäude an. Mit ihrem Dienstausweis wird ihr Einlass in das Gebäude gewährt.

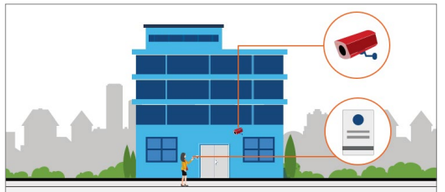
Weiter ...

Die Grundlagen von Zero Trust

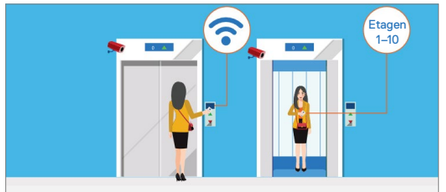
Zero Trust ist eine neue Herangehensweise an das Thema Sicherheit. Es ersetzt das *implizite* Vertrauen, was bedeutete, dass NutzerInnen nach der Authentifizierung im Netzwerk frei handeln können. Zero Trust leitet einen Paradigmenwechsel ein und gibt Unternehmen die explizite Kontrolle über ihre IT-Umgebung.

Wir können Zero Trust mit einem bekannten Konzept verdeutlichen: Sicherheitsprotokollen in Gebäuden.

Sie arbeiten bei einem Unternehmen im Büro. Bei Ihrer Einstellung haben Sie einen Mitarbeiterausweis erhalten und die Sicherheitsprotokolle gelernt. Sie betreten jeden Tag das Gebäude. Überall gibt es Kameras. Sie zeigen Ihren Mitarbeiterausweis an mehreren Stellen vor. An Ihrem Schreibtisch entsperren Sie dann Ihren Computer mit einem Kennwort.



Eine Mitarbeiterin kommt am Bürogebäude an. Mit ihrem Dienstausweis wird ihr Einlass in das Gebäude gewährt.



Mit ihrem Dienstausweis bekommt sie Zugang zu dem Aufzug, der ihrer Etage zugewiesen ist.

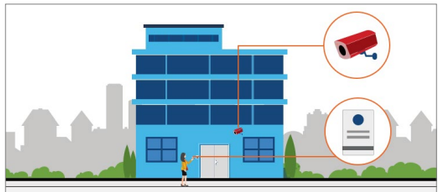
Weiter ...

Die Grundlagen von Zero Trust

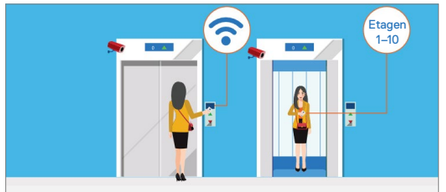
Zero Trust ist eine neue Herangehensweise an das Thema Sicherheit. Es ersetzt das *implizite* Vertrauen, was bedeutete, dass NutzerInnen nach der Authentifizierung im Netzwerk frei handeln können. Zero Trust leitet einen Paradigmenwechsel ein und gibt Unternehmen die explizite Kontrolle über ihre IT-Umgebung.

Wir können Zero Trust mit einem bekannten Konzept verdeutlichen: Sicherheitsprotokollen in Gebäuden.

Sie arbeiten bei einem Unternehmen im Büro. Bei Ihrer Einstellung haben Sie einen Mitarbeiterausweis erhalten und die Sicherheitsprotokolle gelernt. Sie betreten jeden Tag das Gebäude. Überall gibt es Kameras. Sie zeigen Ihren Mitarbeiterausweis an mehreren Stellen vor. An Ihrem Schreibtisch entsperren Sie dann Ihren Computer mit einem Kennwort.



Eine Mitarbeiterin kommt am Bürogebäude an. Mit ihrem Dienstausweis wird ihr Einlass in das Gebäude gewährt.



Mit ihrem Dienstausweis bekommt sie Zugang zu dem Aufzug, der ihrer Etage zugewiesen ist.

Die Mitarbeiterin benutzt ihren Dienstausweis erneut, um die Etagenauswahl im Aufzug zu aktivieren.

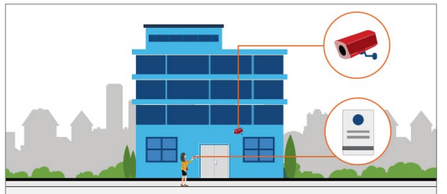
Weiter ...

Die Grundlagen von Zero Trust

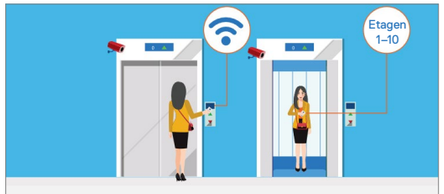
Zero Trust ist eine neue Herangehensweise an das Thema Sicherheit. Es ersetzt das *implizite* Vertrauen, was bedeutete, dass NutzerInnen nach der Authentifizierung im Netzwerk frei handeln können. Zero Trust leitet einen Paradigmenwechsel ein und gibt Unternehmen die explizite Kontrolle über ihre IT-Umgebung.

Wir können Zero Trust mit einem bekannten Konzept verdeutlichen: Sicherheitsprotokollen in Gebäuden.

Sie arbeiten bei einem Unternehmen im Büro. Bei Ihrer Einstellung haben Sie einen Mitarbeiterausweis erhalten und die Sicherheitsprotokolle gelernt. Sie betreten jeden Tag das Gebäude. Überall gibt es Kameras. Sie zeigen Ihren Mitarbeiterausweis an mehreren Stellen vor. An Ihrem Schreibtisch entsperren Sie dann Ihren Computer mit einem Kennwort.

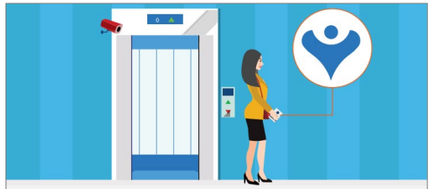


Eine Mitarbeiterin kommt am Bürogebäude an. Mit ihrem Dienstausweis wird ihr Einlass in das Gebäude gewährt.



Mit ihrem Dienstausweis bekommt sie Zugang zu dem Aufzug, der ihrer Etage zugewiesen ist.

Die Mitarbeiterin benutzt ihren Dienstausweis erneut, um die Etagenauswahl im Aufzug zu aktivieren.



Auf der Etage angekommen, begibt sich die Mitarbeiterin zu ihrem Arbeitsplatz.

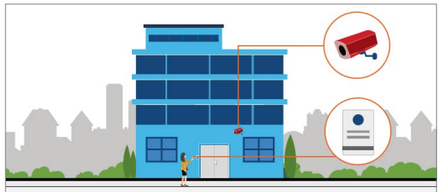
Weiter ...

Die Grundlagen von Zero Trust

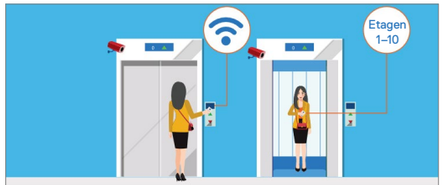
Zero Trust ist eine neue Herangehensweise an das Thema Sicherheit. Es ersetzt das *implizite* Vertrauen, was bedeutete, dass NutzerInnen nach der Authentifizierung im Netzwerk frei handeln können. Zero Trust leitet einen Paradigmenwechsel ein und gibt Unternehmen die explizite Kontrolle über ihre IT-Umgebung.

Wir können Zero Trust mit einem bekannten Konzept verdeutlichen: Sicherheitsprotokollen in Gebäuden.

Sie arbeiten bei einem Unternehmen im Büro. Bei Ihrer Einstellung haben Sie einen Mitarbeiterausweis erhalten und die Sicherheitsprotokolle gelernt. Sie betreten jeden Tag das Gebäude. Überall gibt es Kameras. Sie zeigen Ihren Mitarbeiterausweis an mehreren Stellen vor. An Ihrem Schreibtisch entsperren Sie dann Ihren Computer mit einem Kennwort.

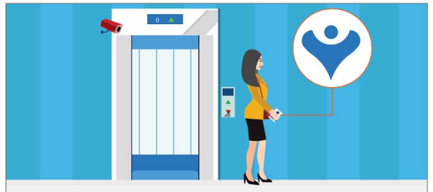


Eine Mitarbeiterin kommt am Bürogebäude an. Mit ihrem Dienstausweis wird ihr Einlass in das Gebäude gewährt.

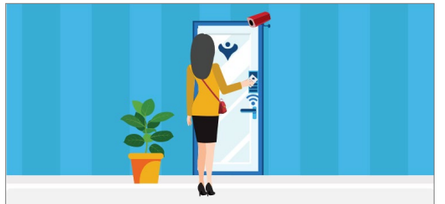


Mit ihrem Dienstausweis bekommt sie Zugang zu dem Aufzug, der ihrer Etage zugewiesen ist.

Die Mitarbeiterin benutzt ihren Dienstausweis erneut, um die Etagenauswahl im Aufzug zu aktivieren.



Auf der Etage angekommen, begibt sich die Mitarbeiterin zu ihrem Arbeitsplatz.



Per Swipe ihrer ID-Karte erhält sie Zutritt zu ihrer Bürosuite.

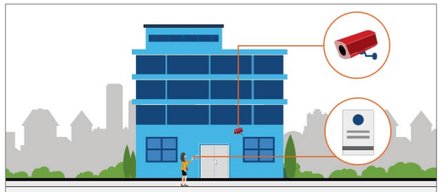
Weiter ...

Die Grundlagen von Zero Trust

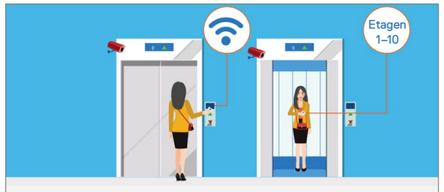
Zero Trust ist eine neue Herangehensweise an das Thema Sicherheit. Es ersetzt das *implizite* Vertrauen, was bedeutete, dass NutzerInnen nach der Authentifizierung im Netzwerk frei handeln können. Zero Trust leitet einen Paradigmenwechsel ein und gibt Unternehmen die explizite Kontrolle über ihre IT-Umgebung.

Wir können Zero Trust mit einem bekannten Konzept verdeutlichen: Sicherheitsprotokollen in Gebäuden.

Sie arbeiten bei einem Unternehmen im Büro. Bei Ihrer Einstellung haben Sie einen Mitarbeiterausweis erhalten und die Sicherheitsprotokolle gelernt. Sie betreten jeden Tag das Gebäude. Überall gibt es Kameras. Sie zeigen Ihren Mitarbeiterausweis an mehreren Stellen vor. An Ihrem Schreibtisch entsperren Sie dann Ihren Computer mit einem Kennwort.

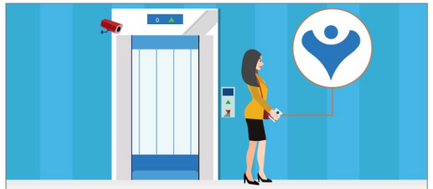


Eine Mitarbeiterin kommt am Bürogebäude an. Mit ihrem Dienstausweis wird ihr Einlass in das Gebäude gewährt.

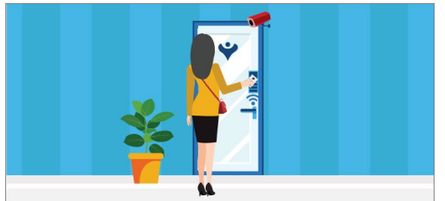


Mit ihrem Dienstausweis bekommt sie Zugang zu dem Aufzug, der ihrer Etage zugewiesen ist.

Die Mitarbeiterin benutzt ihren Dienstausweis erneut, um die Etagenauswahl im Aufzug zu aktivieren.



Auf der Etage angekommen, begibt sich die Mitarbeiterin zu ihrem Arbeitsplatz.



Per Swipe ihrer ID-Karte erhält sie Zutritt zu ihrer Bürosuite.

Die Mitarbeiterin setzt sich an ihren Schreibtisch und entsperrt ihren Computer mit einem Kennwort.

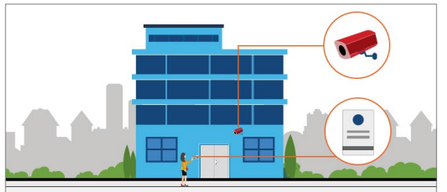
Weiter ...

Die Grundlagen von Zero Trust

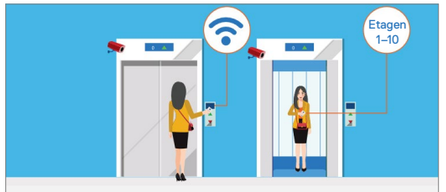
So funktioniert Zero Trust

Ihr Arbeitgeber hat Sie am ersten Tag identifiziert. Jeglicher Zugriff, den Sie seitdem angefordert haben, wurde verifiziert, um die Ressourcen des Unternehmens zu schützen (NutzerInnen, Daten usw.). Für noch mehr Sicherheit überwacht Sicherheitspersonal sämtliche Bewegungen im Gebäude auf Monitoren. Ungewöhnliches Verhalten – z. B. der Versuch, sich Zugang zu einer Suite zu verschaffen, in der Sie nichts zu suchen haben – wird immer untersucht.

NutzerInnen, Geräte, Anwendungen und Daten befinden sich heute häufiger außerhalb des Unternehmensnetzwerks als jemals zuvor. Das hat dazu geführt, dass Nutzeridentitäten zu einer Schwachstelle geworden sind und die Identitätskompromittierung mittlerweile das Kernelement bei den meisten Sicherheitsverletzungen ist. Zero Trust leitet hier eine Kurskorrektur ein.

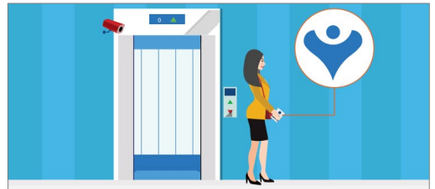


Eine Mitarbeiterin kommt am Bürogebäude an. Mit ihrem Dienstausweis wird ihr Einlass in das Gebäude gewährt.

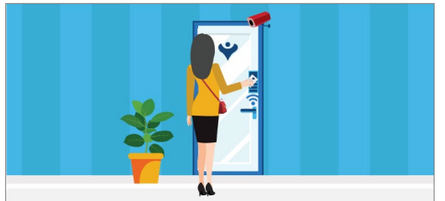


Mit ihrem Dienstausweis bekommt sie Zugang zu dem Aufzug, der ihrer Etage zugewiesen ist.

Die Mitarbeiterin benutzt ihren Dienstausweis erneut, um die Etagenauswahl im Aufzug zu aktivieren.



Auf der Etage angekommen, begibt sich die Mitarbeiterin zu ihrem Arbeitsplatz.



Per Swipe ihrer ID-Karte erhält sie Zutritt zu ihrer Bürosuite.

Die Mitarbeiterin setzt sich an ihren Schreibtisch und entsperrt ihren Computer mit einem Kennwort.

Implementierung von Zero-Trust-Prinzipien

Endpoint Security ist ein kritischer Bestandteil einer Zero-Trust-Transformation.

Für eine effektive Zero-Trust-Strategie müssen Sie die Endpunkte absichern.

Dem MITRE ATT&CK®-Framework zufolge gibt es heute neun „Erstzugriffstechniken“, mit denen Angreifer sich Zugang zu Netzwerken verschaffen *(siehe Abbildung)*.[vi] Untersuchungen zeigen, dass herkömmliche Abwehrmaßnahmen die Sicherheit von Endpunkten in der Cloud-basierten Welt von heute nicht gewährleisten können. Angreifern genügt ein einziges Einfallstor. Bei Endpunkten können Bedrohungsakteure Dutzende von Sicherheitslücken während des gesamten Lebenszyklus eines Geräts ausnutzen.

Je größer die Anzahl an Geräten in einem Netzwerk wird, umso mehr werden Endpunkte zum Angriffsvektor.

Sicherheitsrichtlinien in einem Zero-Trust-Modell definieren das akzeptable Verhalten bis ins kleinste Detail – alles andere wird blockiert. Dann überwacht das Bedrohungsmanagement jegliche Abweichungen vom akzeptablen Verhalten. Ungewöhnliches Verhalten wird gemeldet und die potenziellen Bedrohungen werden durch Einleiten der entsprechenden Korrekturmaßnahmen beseitigt.

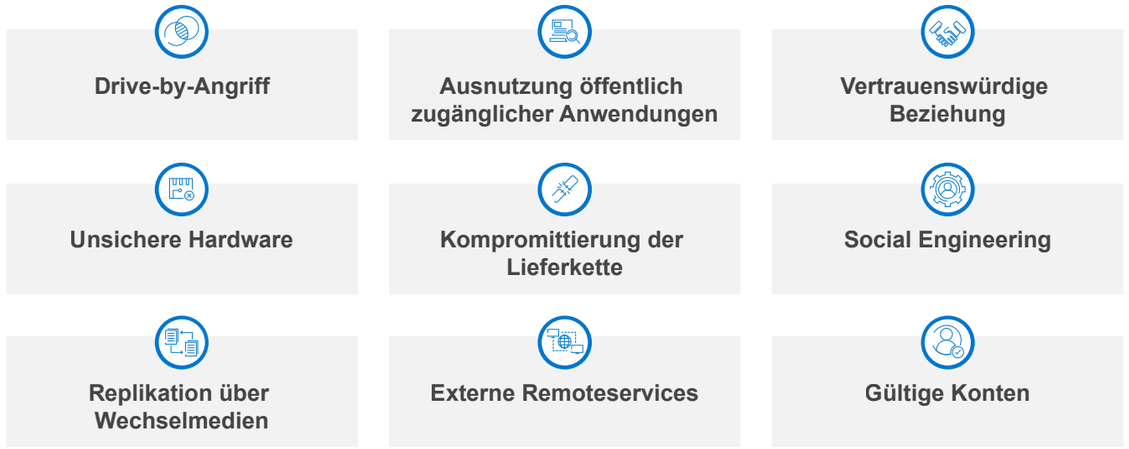


Abbildung 1/3

Implementierung von Zero-Trust-Prinzipien

Endpoint Security ist ein kritischer Bestandteil einer Zero-Trust-Transformation.

Für eine effektive Zero-Trust-Strategie müssen Sie die Endpunkte absichern.

Dem MITRE ATT&CK®-Framework zufolge gibt es heute neun „Erstzugriffstechniken“, mit denen Angreifer sich Zugang zu Netzwerken verschaffen *(siehe Abbildung)*.[vi] Untersuchungen zeigen, dass herkömmliche Abwehrmaßnahmen die Sicherheit von Endpunkten in der Cloud-basierten Welt von heute nicht gewährleisten können. Angreifern genügt ein einziges Einfallstor. Bei Endpunkten können Bedrohungsakteure Dutzende von Sicherheitslücken während des gesamten Lebenszyklus eines Geräts ausnutzen.

Je größer die Anzahl an Geräten in einem Netzwerk wird, umso mehr werden Endpunkte zum Angriffsvektor.

Sicherheitsrichtlinien in einem Zero-Trust-Modell definieren das akzeptable Verhalten bis ins kleinste Detail – alles andere wird blockiert. Dann überwacht das Bedrohungsmanagement jegliche Abweichungen vom akzeptablen Verhalten. Ungewöhnliches Verhalten wird gemeldet und die potenziellen Bedrohungen werden durch Einleiten der entsprechenden Korrekturmaßnahmen beseitigt.

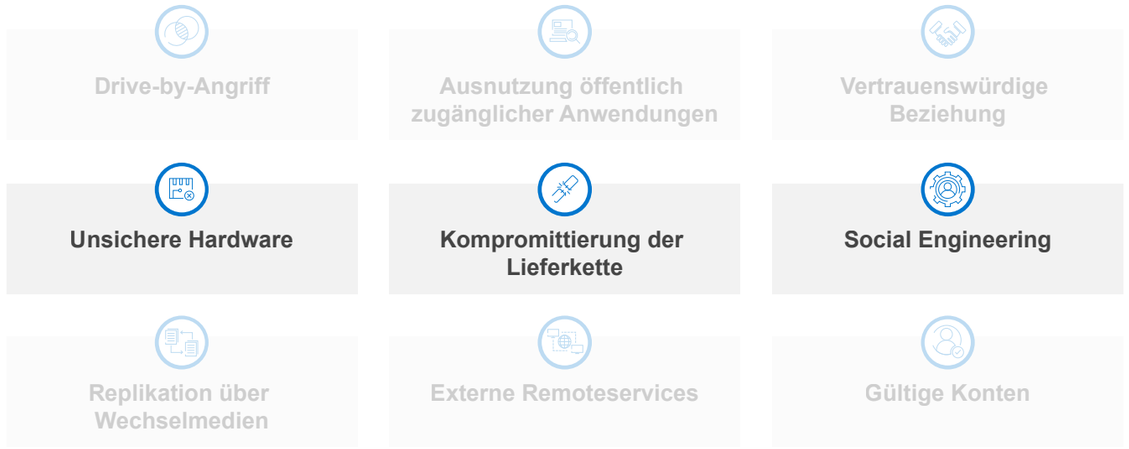


Abbildung 2/3

Implementierung von Zero-Trust-Prinzipien

Endpoint Security ist ein kritischer Bestandteil einer Zero-Trust-Transformation.

Für eine effektive Zero-Trust-Strategie müssen Sie die Endpunkte absichern.

Dem MITRE ATT&CK®-Framework zufolge gibt es heute neun „Erstzugriffstechniken“, mit denen Angreifer sich Zugang zu Netzwerken verschaffen *(siehe Abbildung)*.[vi] Untersuchungen zeigen, dass herkömmliche Abwehrmaßnahmen die Sicherheit von Endpunkten in der Cloud-basierten Welt von heute nicht gewährleisten können. Angreifern genügt ein einziges Einfallstor. Bei Endpunkten können Bedrohungsakteure Dutzende von Sicherheitslücken während des gesamten Lebenszyklus eines Geräts ausnutzen.

Je größer die Anzahl an Geräten in einem Netzwerk wird, umso mehr werden Endpunkte zum Angriffsvektor.

Sicherheitsrichtlinien in einem Zero-Trust-Modell definieren das akzeptable Verhalten bis ins kleinste Detail – alles andere wird blockiert. Dann überwacht das Bedrohungsmanagement jegliche Abweichungen vom akzeptablen Verhalten. Ungewöhnliches Verhalten wird gemeldet und die potenziellen Bedrohungen werden durch Einleiten der entsprechenden Korrekturmaßnahmen beseitigt.

Abbildung 3/3

Drei Empfehlungen zur Umsetzung von Zero Trust

Schaffen Sie in Ihrem Unternehmen die Basis für eine erfolgreiche Zero-Trust-Transformation.

1

Implementierung der richtigen Richtlinien und Kontrollen für Ihre Unternehmensprioritäten

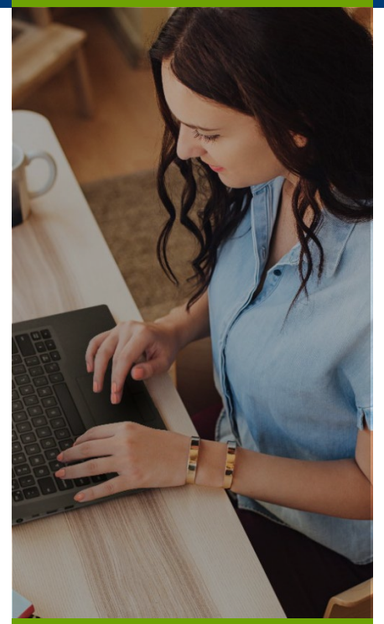
Policy Engines und das Richtlinienmanagement sind für effektive Zero-Trust-Implementierungen entscheidend. Da Unternehmen aber nie ein unbeschränktes Sicherheitsbudget haben, müssen zuerst die Unternehmensprioritäten ermittelt werden. Was möchten Sie in puncto Ressourcen und geistiges Eigentum unbedingt schützen? Gleichen Sie diese Angriffsfläche mit dem zulässigen Risiko Ihres Unternehmens ab.

Überprüfen Sie dann die aktuell vorhandenen Policies und Kontrollen. Die Risiken von heute entspringen der Cloud-basierten Welt, in der wir leben. Wird das bei Ihrer Policy Engine berücksichtigt?

Wenn Sie Policies zum Steuern des Zugriffs auf Ihre wichtigsten Ressourcen implementiert haben, können Sie den Umfang ausweiten.

WEITERE INFORMATIONEN

Weitere Informationen erhalten Sie *in diesem Video*, in dem CybersicherheitsexpertInnen von Dell die wesentlichen Sicherheitsrisiken besprechen, mit denen Unternehmen heute konfrontiert sind.



Da sich mehr NutzerInnen, Anwendungen, Daten und Geräte als jemals zuvor außerhalb des Unternehmensnetzwerks befinden, mussten **82 %** der IT-Entscheidungsträgerinnen eigenen Angaben zufolge ihre Sicherheitsrichtlinien überdenken.[x]

Drei Empfehlungen zur Umsetzung von Zero Trust

Schaffen Sie in Ihrem Unternehmen die Basis für eine erfolgreiche Zero-Trust-Transformation.

2 Sichere Geräte als Basis

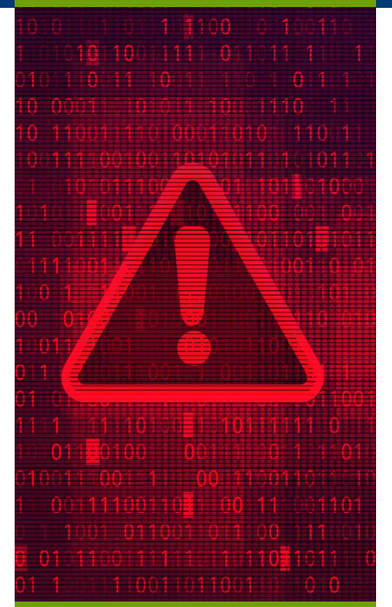
Stützen Sie sich bei der Zero-Trust-Planung auf eine sichere Grundlage. Stärken Sie Ihre Abwehr mit Geräten, bei denen Sicherheit ein wichtiger Aspekt bei Design und Entwicklung war. Dazu gehören:

A. **Hardware- und Firmwarebasierte Schutzfunktionen**, die den Endpunkt-Stack absichern und für Transparenz sorgen (z. B. durch Erkennung eines kompromittierten BIOS und Benachrichtigung der IT). Rüsten Sie Ihr Unternehmen mit Technologien aus, die die Identität bei jeder neuen Zugriffsanfrage überprüfen – und das mit möglichst geringen Auswirkungen auf die Mitarbeiterproduktivität.

B. **Lieferketten-Schutzfunktionen und Integritätskontrollen**, die jeden Schritt im PC-Lebenszyklus absichern. Wir haben in den letzten Jahren gesehen, dass Lieferkettenangriffe verheerend sein können. Bei einer echten Zero-Trust-Architektur beginnen Authentifizierung, Verifizierung und Monitoring bei der Lieferkette. Arbeiten Sie mit Anbietern zusammen, die 1) sichere Praktiken einsetzen und 2) es Ihnen ermöglichen, die Integrität Ihrer Geräte zu validieren – von der Beschaffung über die Fertigung bis hin zur Bereitstellung.

WEITERE INFORMATIONEN

Weitere Informationen zu Best Practices für Gerätesicherheit finden Sie im Whitepaper von Dell und Intel mit dem Titel Achieving Pervasive Security Above and Below the OS.



Im Jahr **2021** hat ein IT-Management-Unternehmen einen Ransomware-Angriff an mindestens **1.500** Kunden weitergetragen.[xi]

Drei Empfehlungen zur Umsetzung von Zero Trust

Schaffen Sie in Ihrem Unternehmen die Basis für eine erfolgreiche Zero-Trust-Transformation.

3

Das Ziel: nahtlose Integration und Interoperabilität in Ihrer Umgebung

Zum Erreichen eines effektiven Sicherheitsstatus sind auf übergeordneter Ebene drei Dinge wichtig:

A. Integration aller Abwehrmaßnahmen in der gesamten IT-Umgebung

B. Transparenz in Echtzeit

C. Bei Bedarf Möglichkeit zum Ergreifen von Maßnahmen

In unserer Cloud-basierten Welt, in der selbst die kleinste ungeprüfte Sicherheitslücke zu einem Albtraum führen kann, ist es wichtig, dass alle Systeme potenzielle Bedrohungen erkennen *und* imstande sind, die nötigen Maßnahmen einzuleiten.

Sind Ihre Systeme integriert oder agieren sie in Silos? Kann Ihre Policy Engine einen bestimmten Workflow anstoßen, wenn ein/e IT-AdministratorIn über ein korrumpiertes BIOS im Netzwerk benachrichtigt wird? In einer integrierten Umgebung sollten automatisierte Prozesse jedes betroffene BIOS unmittelbar unter Quarantäne stellen, jeden weiteren Zugriff beschränken und einen Patching-Durchlauf ausführen.

Wie steht es um transparente Einblicke in alle Ihre Endpunkte? Idealerweise verfügen Sie über umfangreiche Telemetrie auf allen Ebenen, von der Lieferkette (z. B. der Laderampe) bis hin zur Firmware (z. B. Warnmeldungen bei versuchter BIOS-Manipulation)

Diese Telemetrie ist aber nur so gut wie Ihre Integrationen. Können Sie auf Basis Ihrer Daten handeln? Es ist wichtig, über die richtigen Ressourcen, wie z. B. fähige CybersicherheitsexpertInnen, zu verfügen, damit die Daten und Programmworkflows zum Bewältigen von Problemen sinnvoll eingesetzt werden können.

41 % der Unternehmen setzen auf Zero Trust.[xii]

DELL Technologies

Entscheidende Punkte

Zero Trust ist im Bereich Sicherheitsstrategie zukunftsweisend

- Mit den neuen Gegebenheiten in der Arbeitswelt haben die Angriffsvektoren zugenommen.
- Sicherheitsverletzungen sind unvermeidlich. Minimieren Sie die Angriffsfläche mit Abwehrmaßnahmen, die für das Worst-Case-Szenario ausgelegt sind.
- Zero Trust ist eine neue Herangehensweise an das Thema Sicherheit, mit der Unternehmen die explizite Kontrolle über die IT-Umgebung erhalten.
- Um eine sichere, moderne Basis aufzubauen, sind Funktionen zum Schutz von Endpunkten erforderlich, die Zero-Trust-Anforderungen erfüllen.
- Identifizieren Sie Ihre wichtigsten Ressourcen bei der Erstellung Ihrer Zero-Trust-Architektur und priorisieren Sie diese entsprechend.
- Kaufen Sie Geräte von Anbietern, die integrierte Schutzfunktionen bieten und stark in ihre Lieferkettenkontrollen investieren.
- Bewerten Sie die Sicherheit und die IT-Interoperabilität. Arbeiten Sie weiter an der Integration von Workflows zum Stärken Ihres Sicherheitsstatus.

Ihr nächster Schritt

Das Thema Sicherheit ist für Unternehmen jeder Größe eine echte Herausforderung. Setzen Sie auf einen erfahrenen Sicherheits- und Technologiepartner, der Sie beim Optimieren Ihrer Zero-Trust-Transformation unterstützen kann.

Dell Trusted Workspace trägt zur Absicherung von Endpunkten bei, damit Sie eine moderne, Zero Trust-fähige IT-Umgebung aufbauen können. Verkleinern Sie die Angriffsfläche mit einem umfassenden Portfolio an Schutztechnologie für Hardware und Software, exklusiv von Dell. Unser rundum koordinierter, abwehrbasierter Ansatz entschärft Bedrohungen, indem integrierte Schutzmaßnahmen mit kontinuierlicher Wachsamkeit kombiniert werden. Unsere Sicherheitslösungen wurden für die Cloud-basierte Welt von heute konzipiert und sorgen für Produktivität seitens der EndnutzerInnen und eine starke IT.

Kontaktieren Sie uns: EndpointSecurity@Dell.com

Besuchen Sie uns unter: Dell.com/Endpoint-Security

Folgen Sie uns: LinkedIn @DellTechnologies | Twitter @DellTech

DELL Technologies

[i] Cybersecurity Almanac, 2. Edition. Cybersecurity Ventures, 2022 https://cybersecurityventures.com/cybersecurity-almanac-2022/

[ii] Ponemon Institute und IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach

[iii] American College of Cardiology, You Will Be Hacked. Plan Now: Cybersecurity in Health Care, 2021 https://www.acc.org/Latest-in-Cardiology/Articles/2021/11/01/01/42/Feature-You-Will-Be-Hacked-Plan-Now-Cybersecurity-in-Health-Care

[iv] Ponemon Institute und IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach

[v] ESG Complete Survey Results: Security Hygiene and Posture Management, 2022 https://www.esg-global.com/research/esg-complete-survey-results-security-hygiene-and-posture-management

[vi] MITRE ATT&CK https://attack.mitre.org/tactics/TA0001/

[vii] Futurum, Four Keys to Navigating the Hardware Security Journey, 2020 https://futurumresearch.com/research-reports/four-keys-to-navigating-the-hardware-security-journey/

[viii] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[ix] Verizon Data Breach Investigations Report, 2022 https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

[x] Absolute Endpoint Risk Report, 2021 https://www.absolute.com/go/reports/endpoint-risk-report/

[xi] TechTarget, 2021 https://www.techtarget.com/searchsecurity/news/252503605/Kaseya-1500-organizations-affected-by-REvil-attacks

[xii] Ponemon Institute und IBM, Cost of a Data Breach Report, 2022 https://www.ibm.com/security/data-breach