FORESCOUT

DIE ROLLE DER IT-SICHERHEIT BEI DER PRÜFUNG VON FUSIONEN & ÜBERNAHMEN

Eine Forschungsstudie zum besseren Verständnis von IT-Sicherheitsrisiken, denen Unternehmen bei der Übernahme anderer Firmen ausgesetzt sind.

ZIEL DER STUDY

Diese Studie wurde erstellt, um die wachsende Bedeutung von Cyber-Risiken und Bewertung von Sicherheitsprüfungen bei Fusionen und Übernahmen (Mergers & Acquisitions, M&A) zu untersuchen. Außerdem galt es festzustellen, wie gut Unternehmen aus Sicht von IT-Entscheidern (IT Decision Makers, ITDMs) und Business-Entscheidern (Business Decision Makers, BDMs) auf den Umgang mit Cyber-Risiken bei M&As vorbereitet sind.

Sind wichtige Entscheidungsträger während einer Akquisition über die Internetsicherheit besorgt? Welche Faktoren werden im Rahmen der Due Diligence und der Bewertung vor, während und nach der Akquisition berücksichtigt? Führen Cyber-Angriffe zu Verzögerungen bei der Akquisition? Welche Bedeutung haben Cyber-Risiken für Unternehmen, die eine Akquisition anstreben? Wie können diese sich selbst in diesem wichtigen Prozess am besten schützen, um Risiken zu minimieren und ihr Unternehmen zu schützen? Dieser Bericht untersucht diese und weitere Fragen und gibt Empfehlungen für ein effektives Management von IT-Sicherheitsrisiken während einer Akquisition.

Forescout Technologies hat diese Studie und Bericht in Auftrag gegeben. Die Befragten wurden von Quest Mindshare rekrutiert.

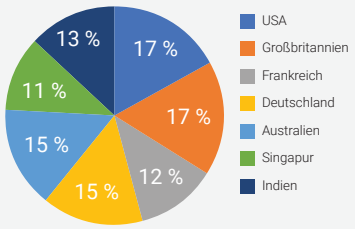
ÜBER DIE STUDIE

Dieser Bericht basiert auf einer Umfrage, die vom 20. Februar bis 10. März 2019 im Auftrag von Forescout Technologies von Quest Mindshare mit Befragten durchgeführt wurde, um das Cyber-Risiko während der Durchführung einer Übernahme besser zu verstehen. Insgesamt wurden 2.779 Personen weltweit befragt, die sich in die zwei Gruppen IT-Entscheider (ITDMs; n=1.283) und Business-Entscheider

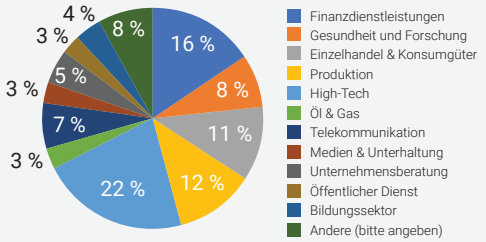
(BDMs; n=1.496) aufteilen. Die Daten wurden gewichtet, um Zielgruppen und Regionen gleichwertig darzustellen. Um sich zu qualifizieren, mussten die Befragten Vollzeitbeschäftigte, mindestens Senior Manager und primäre Entscheider für IT-Einkäufe oder in die M&A-Strategie involviert sein. Die Umfrage wurde in den Vereinigten Staaten, Frankreich, Großbritannien, Deutschland, Australien, Singapur und Indien durchgeführt. Die Fehlerquote beträgt +/- 1,73 Prozentpunkte.

Verteilung der Befragten

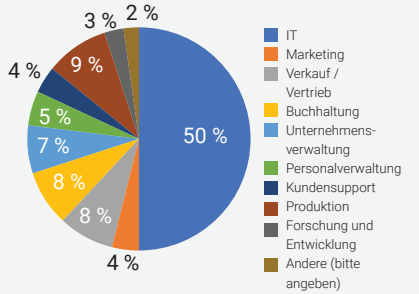
Länder



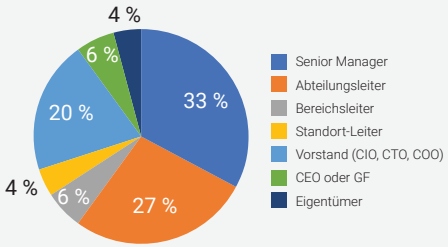
Branchen



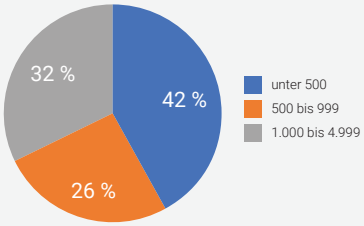
Tätigkeit



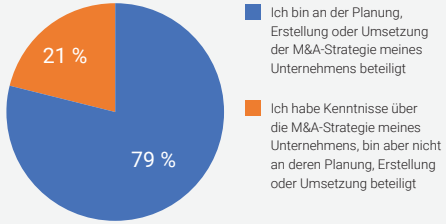
Management-Level



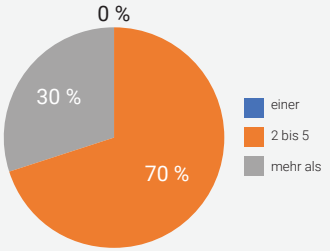
Anzahl Beschäftigte

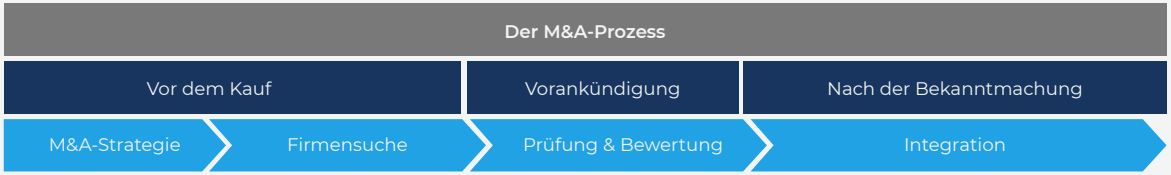


Grad der Beteiligung



An wie vielen M&As beteiligt





ZUSAMMENFASSUNG

Gartner postuliert für 2022, dass 60 % der Unternehmen mit M&A-Aktivitäten die Cybersicherheit als kritischen Faktor1 in ihrem Due-Diligence-Prozess betrachten werden – heute sind es weniger als 5 %. In unserer Umfrage unter weltweit 2.779 IT- und Business-Entscheidern bejahten 73 %, dass die Technologieakquisition oberste Priorität für ihre M&A-Strategie im nächsten Jahr hat – und 62 % meinten, dass ihr Unternehmen durch die Übernahme neuer Unternehmen einem erheblichen IT-Sicherheitsrisiko ausgesetzt ist. Auch nach dem Kauf bleibt es die größte Gefahr.

Während Unternehmen bei einem Deal Rückfallklauseln respektieren, kennt Malware sowas nicht. Einmal verbunden haben böse Akteure freie Hand, es sei denn, Sie sind darauf vorbereitet.

Das IT-Sicherheitsrisiko ist aus mehreren Gründen eine wachsende Herausforderung. Menschliches Versagen ist ein uralter Netzwerkteufel. Menschliche Fahrlässigkeit und Neugierde sind die am häufigsten genannten Gründe2 für ein Sicherheitsproblem. Die IT- und Cyberlandschaft hat sich in den letzten Jahrzehnten jedoch dramatisch verändert – mit neuen Vorteilen, aber auch neuen Risiken. Auch die Einführung des Internet der Dinge (Internet of Things, IoT) hat die Art, wie Menschen leben und kommunizieren, verändert. Bis 2023 wird es voraussichtlich mehr als 20,4 Mrd. IoT-Geräte geben, was ein innovatives Management von IoT-Cyber-Risiken erfordert. In unserer Umfrage bewerteten 72 % der Befragten IoT-Geräte (Drucker, smarte Beleuchtung, VoIP-Telefone, Videokameras) als besonders anfällig für Angriffe von außen. IoT-Geräte haben das fortschreitende Zusammenwachsen von IT und operative Technologien (Operational Technology, OT) befördert und Produktionsnetzwerke integriert, die bisher schwer anzugreifen waren

In den letzten Jahren gab es viele Veränderungen und Weiterentwicklungen, die auch potenziellen Angreifern mehr Möglichkeiten geben, böswillige Angriffe zu starten, Daten und Wissen zu stehlen oder zu versuchen, ein Geschäft oder die Wirtschaft zu stören. All diese Faktoren haben den Bewertungs- und Entscheidungsprozess von ITDMs und BDMs im Bereich M&A erheblich erschwert. Sie stellen spezielle Cyber-Risiken dar, die bewertet werden müssen. Und sie sind auch schwer zu bewerten, da viele Assets nicht inventarisiert werden. Eine überstürzte, uninformierte oder

M&A-Strategie für die nächsten 12 Monate

73 %

stimmten zu, dass die Technologieakquisition für ihre M&A-Strategie in den nächsten 12 Monaten oberste Priorität hat.

62 %

gaben an, dass ihr Unternehmen einem erheblichen IT-Sicherheitsrisiko ausgesetzt ist, wenn es neue Unternehmen erwirbt, und dass das Cyber-Risiko danach ihr größtes Anliegen ist.

[1] *Cybersecurity is Critical to the M&A Due Diligence Process (Cybersicherheit ist ein kritischer Faktor im M&A Due-Diligence-Prozess), Gartner,* April 2018, https://www.gartner.com/en/documents/3873604

[2] *The biggest cybersecurity risk to US businesses is employee negligence (Das größte Cybersicherheits-Risiko für US Unternehmen ist die Fahrlässigkeit von Mitarbeitern), CNBC,* Juni 2018, https://www.cnbc.com/2018/06/21/ the-biggest-cybersecurity-risk-to-us-businesses-is-employee- negligence-study-says.html

[3] *8.4 Billion Connected "Things" Will be in Use in 2017 (8,4 Mrd. vernetzte "Dinge" werden in 2017 in Gebrauch sein),* https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connectedthings-will-be-in-use-in-2017-up-31-percent-from-2016

begrenzte Bewertung kann heftige finanzielle Auswirkungen sowohl für das kaufende als auch das übernommene Unternehmen haben. Beispiele dafür sind die nachträgliche Kaufpreissenkung um 292 Mio. € 4 nach der Offenlegung von Yahoo's Sicherheitsverletzungen sowie die 1,25 Mio. € für den Vergleich von Datenschutzverletzungen5, den der Einzelhändler Neiman Marcus in den USA nach der Übernahme zahlen musste.

Eine Due Diligence konzentriert sich traditionell u.a. auf Finanzen, Recht, Vertrieb, Produktion, Personal und IT. Unsere Umfrageergebnisse zeigen, dass Unternehmen mit Kaufabsichten, gerade dann von einer großen dedizierten Sicherheitsprüfung profitieren können, wenn sie während der Akquisition Cyber-Risiken erkennen. Unsere Erkenntnisse machen deutlich, dass die Prüfung einer Akquisition keine einmalige Aufgabe ist; die Prüfung der IT-Sicherheit und eine Risikobewertung sollten fortlaufende Aktivitäten sein. Dennoch können akquirierende Unternehmen bei ihren Prüfungen und Untersuchungen oft nicht so weit gehen - daher bleibt bei jeder Akquisition ein gewisses Restrisiko. Sie wissen nie wirklich, was Sie kaufen, bis Sie es integrieren - und das macht es umso wichtiger, so viel wie möglich vor der Integration herauszufinden. Während Unternehmen bei einem Deal Rückfallklauseln respektieren, kennt Malware sowas nicht. Einmal verbunden haben böse Akteure freie Hand, es sei denn, Sie sind darauf vorbereitet.

[4] *Verizon cuts Yahoo deal price by $350 million (Verizon senkt den Yahoo-Kaufpreis um 292 Mio Euro),* CNN, Februar 2017, https://money.cnn.com/2017/02/21/technology/yahoo-verizon-deal/index.html

[5] *Neiman Marcus to pay $1.5M settlement over 2013 data breach (Neiman Marcus zahlt 1,25 Mio. Euro für Datenverstöße in 2013), RetailDive,* Januar 2019, https://www.retaildive.com/news/neiman-marcus-to-pay-15m-settlement-over-2013-data-breach/545641/

DIE WICHTIGSTEN ERKENNTNISSE

- **IT-Sicherheitsprobleme gibt es häufig und sie können einen Deal torpedieren:** Mehr als die Hälfte der Befragten (53 %) berichten, dass sie während einer M&A-Transaktion auf kritische Sicherheitsvorfälle gestoßen sind, die den Kauf gefährdeten.
- **Unternehmen legen mehr Wert auf die Cybersicherheit eines Ziels als bisher:** 81 Prozent der ITDMs und BDMs sind sich einig, dass sie sich mehr als früher auf die Sicherheit eines Kandidaten konzentrieren und betonen, dass Sicherheit oberste Priorität sowohl für IT- als auch für Business-Entscheider hat.
- **Ein verheimlichtes Sicherheitsproblem ist für die meisten Unternehmen ein No-Go:** 73 Prozent der Befragten stimmten zu, dass nicht offengelegte Datenverstöße sofort zum Abbruch des M&A-Deals führen.
- **Entscheider haben öfter das Gefühl, nicht genügend Zeit für eine Cyber-Evaluierung zu haben:** Nur 36 % der Befragten meinen, dass ihr IT-Team die Cybersicherheitsstandards, -prozesse und -protokolle des Unternehmens ausreichend überprüfen kann, bevor sie es übernehmen.
- **Internen IT-Teams können die Fähigkeiten für die Beurteilung der IT-Sicherheit fehlen:** Von den ITDMs sind nur 37 % der Befragten überzeugt, dass ihr IT-Team über die notwendigen Fähigkeiten verfügt, um eine Cybersicherheitsbewertung für eine Akquisition durchzuführen.
- **Unternehmen nutzen externe Ressourcen für IT-Sicherheitsüberprüfungen:** Fast alle Befragten (97 %) gaben an, dass ihre Unternehmen Geld für externe Dienstleister für IT-Audits oder Sicherheitsrisikobewertungen ausgeben.
- **Vernetzte Geräte und menschliche Fehler setzen Unternehmen Risiken aus:** Gefragt, was Unternehmen während des Informations- und Technologieprozesses am meisten gefährdet, stachen zwei Antworten hervor: menschliche Fehler und Konfigurationsschwächen (51 %) und vernetzte Geräte (50 %).
- **Geräte werden bei einer Integration oft übersehen:** Mehr als die Hälfte (53 %) der ITDMs geben an, dass nach der Integration einer neuen Akquisition Geräte nicht erfasst wurden.
- Das Übersehen von Cyber-Risiken kann heftige Folgen haben: 65 % der Befragten gaben an, dass ihre Unternehmen es aus Cybersicherheitsgründen bereuen, einen M&A-Deal getätigt zu haben.

AKTUELLE CYBERSICHERHEITSLAGE BEI M&A

IT-Sicherheitsprobleme gibt es häufig und sie können einen Deal torpedieren:

53 %

53 % der Befragten berichteten, dass sie während einer M&A-Transaktion auf kritische Sicherheitsvorfälle gestoßen sind, die den Kauf gefährdeten.

US	UK	FR	DE	AUS	SG	IN
47 %	52 %	61 %	56 %	40 %	50 %	63 %

Für Unternehmensfusionen und -Käufe gibt es viele Gründe: Mehr Effizienz, Zugang zu größeren Märkten, einzigartiges Know-how, Wettbewerbsvorteile oder Einfluss auf die Lieferkette, um nur einige zu nennen. Egal, ob es sich bei der Übernahme um einen Mischkonzern, eine Markt- oder Produktakquisition oder eine horizontale oder vertikale Fusion handelt, widmet sich der Due-Diligence-Prozess den Bereichen Finanzen, Recht, Wirtschaft, Operations, Personal und IT.

Dieser Prozess erlaubt eine ordentliche Einsicht und Bewertung der Risiken. Doch schon bei kleinen Fusionen machen die vielen Risikofaktoren den Entscheidungsprozess schwierig. Und die wachsende Zahl von Cyber-Risiken erschwert die Sache zusätzlich – die Bewertung der digitalen Assets erfordert das Erfassen der nahezu unsichtbaren belasteten Sicherheitshistorie des Unternehmens. Angesichts dieser Komplexität verwundert es nicht, dass 53 % der Befragten angaben, während einer M&A-Transaktion auf kritische Sicherheitsvorfälle gestoßen zu sein, die den Kauf gefährdeten. Zusätzlich zeigt die Studie:

- IT-Entscheider berichteten häufiger, dass ihr Unternehmen auf einen kritischen, gefährlichen Vorfall gestoßen war (57 %), als Business-Entscheider (48 %).
- Befragte in Frankreich (61 %) und Indien (63 %) berichteten am häufigsten von IT-Sicherheitsproblemen oder Vorfällen.
- Große Unternehmen (mehr als 5.000 Mitarbeiter) (59 %) und mittelständische Unternehmen (1.000 bis 4.999 Mitarbeiter) (56 %) hatten häufiger Cybersicherheitsprobleme als kleinere Firmen mit weniger als 1.000 Mitarbeitern (49 %).

Unsere Ergebnisse zeigen, dass je häufiger eine Person an Fusionen und Übernahmen beteiligt ist, desto eher berichtet sie, dass ihr Unternehmen auf ein kritisches IT-Sicherheits-problem gestoßen ist, das eine M&A-Transaktion gefährdet.

- Auch bei Befragten aus Finanzdienstleistungen (56 %) und High-Tech (57 %) war die Wahrscheinlichkeit höher, dass sie auf ein IT-Sicherheitsproblem gestoßen sind als in anderen Branchen.
- Personen, die an mehr als fünf Fusionen beteiligt waren, gaben eher an, dass ihr Unternehmen auf ein kritisches Cybersicherheitsproblem gestoßen war, das eine M&A-Transaktion gefährdete (60 %), als Befragte mit zwei bis fünf Fusionen (43 %).
- Befragte erfahrener Unternehmen, die zur Abwehr von Cybersicherheitsrisiken mehr Aufwand betreiben, hatten später seltener ein Sicherheitsproblem (46 %). Das deutet darauf hin, dass Kontrollen eine wichtige Rolle bei der Verringerung des Cybersicherheitsrisikos spielen.

Personen, die an mehr als fünf Fusionen beteiligt waren, sagten eher, dass ihr Unternehmen auf ein kritisches IT-Sicherheitsproblem gestoßen war, das eine M&A-Transaktion gefährdete

60 %

Personen, die in 2 bis 5 Fälle involviert waren

43 %

Personen, die in mehr als 5 Fälle involviert waren

PRÜFUNG & BEWERTUNG

Unternehmen legen mehr Wert auf die Cybersicherheit einer Firma als früher:

81 %

81 Prozent bestätigen, dass sie einen stärkeren Fokus auf die Cyber-Sicherheit einer Firma legen als früher.

US	UK	FR	DE	AUS	SG	IN
84 %	77 %	79 %	72 %	73 %	85 %	94 %

Cyber-Risiken in der M&A Due Diligence bewerten

Fast alle Befragten (93 %) gaben an, dass sie IT-Sicherheitsbewertungen als wichtig für die M&A-Entscheidung ihres Unternehmens ansehen.

Wenig überraschend schätzen ITDMs Cyber-Sicherheitsbewertungen häufiger (71 %) als sehr wichtig ein als BDMs (64 %). Aber es ist bemerkenswert, dass beide Zielgruppen diese Bewertungen als einen wichtigen Teil des M&A-Prozesses ihres Unternehmens betrachten.

hat der Erwerb von Technologien in den nächsten 12 Monaten höchste Priorität.

Cybersecurity spielt in der M&A-Strategie eine größere Rolle als bisher, und kann manchmal sogar einen Deal verhindern.

73 % der Befragten erklärten, dass die firmeneigene M&A-Strategie beim Verheimlichen von Sicherheitsproblemen in der Zielfirma einen sofortigen Abbruch vorsieht.

73 % der Befragten erklärten, dass die firmeneigene M&A-Strategie beim Verheimlichen von Sicherheitsproblemen in der Zielfirma einen sofortigen Abbruch vorsieht.

Unternehmen nehmen die Gefährdung durch potenzielle Cyber-Sicherheitsrisiken sehr ernst. 83 % stimmen zu, dass sie die IT-Sicherheitslage einer Zielfirma besonders prüfen, wenn sie ihre Due-Diligence durchführen. Mehr noch, 81 % bestätigen, dass sie sich mehr als in der Vergangenheit auf die Cybersicherheit einer Zielfirma konzentrieren.

Da die digitale Transformation in Firmen immer wichtiger wird, haben eine digitale Strategie und Technologieakquisition für kaufwillige Unternehmen zunehmend an Bedeutung gewonnen. 97 % der Befragten geben an, dass die digitale Strategie in den nächsten 12 Monaten an erster Stelle steht; für 77 %

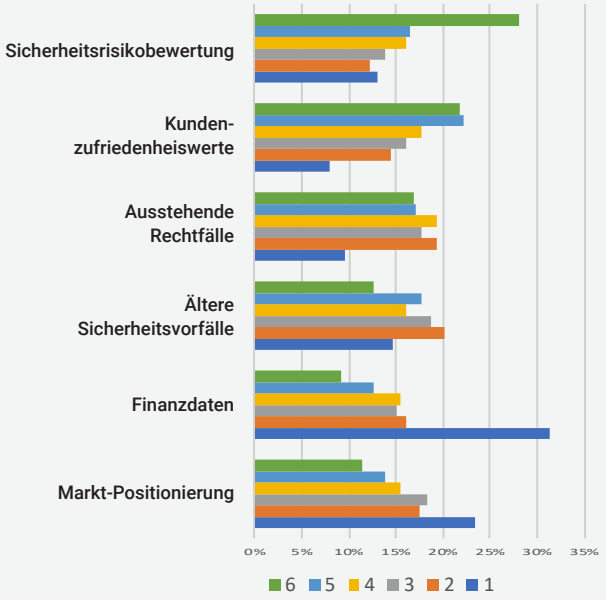
Kritische Due-Diligence-Faktoren

Nach den wichtigsten Faktoren ihres Unternehmens bei einer Due Diligence von Zielfirmen gefragt, war den Personen der Finanzbericht am wichtigsten. Als zweitwichtigsten Faktor nannten sie vergangene Sicherheitsvorfälle, wie in der Grafik rechts dargestellt (1 = sehr wichtig, 6 = unwichtig). Sicherheitsprobleme spielen in den Köpfen der Personen, die die Firmen prüfen und Käufe abschließen, also eine große Rolle.

Auch wenn vergangene Sicherheitsprobleme auf Platz 2 der Liste rangieren, ist es dennoch wichtig zu untersuchen, wie alte und potenzielle Bedrohungen in einer Due Diligence bewertet werden.

Ergebnisse der Frage: Was sind die wichtigsten Faktoren, wenn Ihr Unternehmen eine Due Diligence durchführt (nach Wichtigkeit geordnet)?

1. Finanzdaten
2. Ältere Sicherheitsvorfälle
3. Marktpositionierung
4. Ausstehende Rechtsfälle
5. Kundenzufriedensheitswerte
6. Sicherheitsrisikobewertung



Prozentsatz der Befragten die die Faktoren von sehr wichtig (1) bis unwichtig (6) einschätzen.

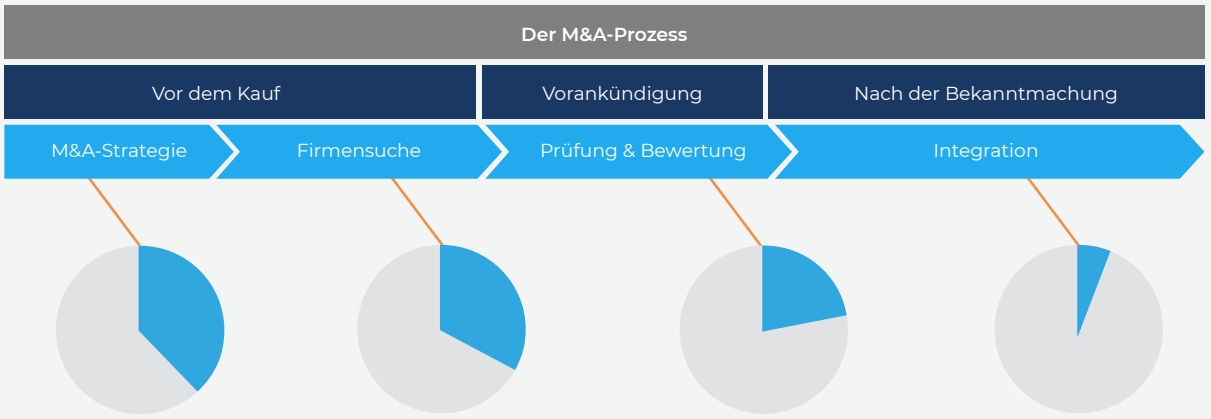
Durchführung einer Due Diligence

Eine M&A Cyber-Due-Diligence umfasst meist interne und externe Evaluierungen. Fast alle Befragten (97 %) gaben an, dass ihre Unternehmen Geld für externe Auftragnehmer ausgeben. 57 % der Befragten bestätigten, dass ihre Firma einen der vier größten Audit-Firmen für Sicherheits-Audits engagiert. Und 80 % antworteten, dass ihr Unternehmen vor der Akquisition eine eingehende interne Inspektion aller IT-Systeme und -Geräte durchgeführt hat.

Diese Ergebnisse zeigen, dass auch in Fällen ohne die vier größten Auditors die meisten Unternehmen zumindest eine interne Bewertung durchführen oder externe Prüfer zur Bewertung einsetzen. Es ist allerdings auch wichtig, den Ansatz der zur Ausführung der Due Diligence und Bewertung verwendet wird, in Betracht zu ziehen.

Security-Assessments sollten ein wichtiger Teil der Akquisitionsbewertung sein - nicht nur während der Integration, sondern der gesamten Akquisition. Dennoch gaben 6 % der Befragten an, dass erst zum Schluss der Akquisition – bei der Integration – die Sicherheitsbewertung begann.

Gefragt, in welcher Phase die IT-Sicherheitsbewertung stattfindet, berichteten die Befragten:



38 % sagten, dass sie mit der Strategie beginnt

33 % sagten, dass sie mit der Firmensuche beginnt

22 % sagten, dass sie mit der Prüfung beginnt

6 % sagten, dass sie mit der Integration beginnt

22 % gaben an, dass sie während der Due Diligence damit begonnen haben, 33 % starteten während des Target Screenings damit, und bei nur 38 % war es Teil der Strategieentwicklung – starteten also zu Beginn des Übernahmeprozesses. Diese Ergebnisse zeigen nicht nur sehr verschiedene Ansichten über den Start einer Sicherheitsbewertung, sondern lassen auch vermuten, dass viele sie nur als eine punktuelle Übung betrachten. Absolut entscheidend ist, dass

> Absolut entscheidend ist, dass die Bewertung des Sicherheitsstandards einer Zielfirma und potenzieller Schwachstellen zu Beginn des M&A-Prozesses startet und sich bis zur Zeit nach der Integration fortsetzt.

die Bewertung des Sicherheitsstandards einer Zielfirma und potenzieller Schwachstellen zu Beginn des M&A-Prozesses startet und sich auch nach der Integration fortsetzt. Auch wenn die erste Bewertung keine signifikanten Cyber-Risiken feststellt, sollte man stets bedenken, das Zielunternehmen während

Entscheider haben öfter das Gefühl, nicht genügend Zeit für Sicherheitsüberprüfungen zu haben:

36 %

Nur 36 % stimmen absolut zu, dass ihr IT-Team genug Zeit hat, um die IT-Sicherheitsstandards, -prozesse und -protokolle der Zielfirma zu überprüfen, bevor der Deal stattfindet.

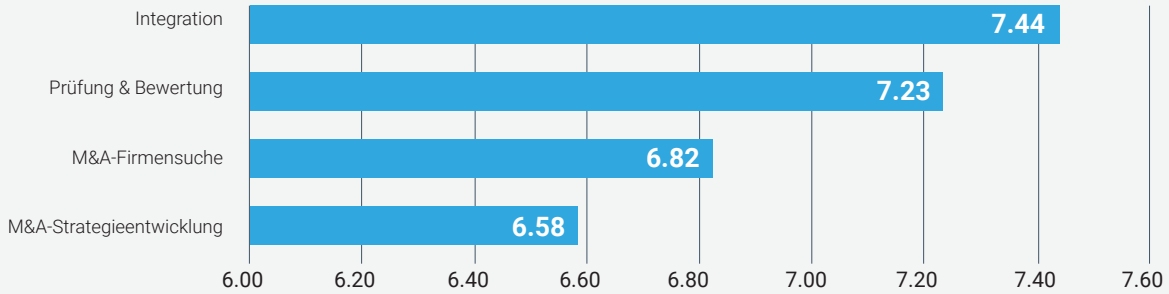
der gesamten Akquisition weiterhin mit Mitarbeitern, Kunden, Lieferanten und der vernetzten Welt zu tun hat.

Die Verwundbarkeit der Unternehmens-Assets kann sich jederzeit erhöhen. Trotz kontinuierlicher Evaluierung kann es sehr schwierig sein, alle Cyber-Risiken dauerhaft im Auge zu behalten.

Gefragt danach, wie groß die Sorge bei ITDMs und BDMs um das IT-Sicherheitsrisiko in jeder Phase des M&A-Prozesses auf einer Skala von 1 bis 10 ist, gab es interessanterweise mehr Bedenken bezüglich der Integration (7,44) als in den Bereichen Prüfung & Evaluierung, (7,23), M&A-Firmensuche (6,82) sowie M&A-Strategieerstellung (6,58).

Ein Wert von 10 steht für größte und eine 1 für keine Besorgnis. Wie bereits gesagt, eine IT-Sicherheitsprüfung sollte sich über die gesamte Akquisition erstrecken, wobei jeder Phase eine besondere Bedeutung zukommt.

Antworten auf die Frage, wie groß ihre Sorge um das IT-Sicherheitsrisiko in jeder Phase des M&A-Lebenszyklus ist.



Um das Risko-Level der Systeme und Prozesse während der Prüfung- und Evaluierungsphase zu bestimmen, betrachten ITDMs und BDMs am häufigsten die IT-Infrastruktur und IT-Lieferkette (54 %), Ergebnisse interner IT-Sicherheitsaudits (48 %), sowie vergangenen Sicherheitsvorfälle (46 %). Am seltensten werden GRC-Systeme (37 %), Patch-Prozesse (36 %) und SIEM (27 %) untersucht. Unternehmen, die mehr als nur ein oder zwei Systeme und Prozesse prüfen, haben auch besser entwickelte M&A-Strategien für Cybersicherheitsrisiken. Diese Kontrollmaßnahmen können eine sehr wichtige Rolle bei der Erfassung und Reduzierung von IT-Sicherheitsrisiken spielen.

Eine gute Bewertung kostet Zeit

Wenn der Druck steigt, Akquisitionen schneller abzuschließen, spielt Zeit eine entscheidende Rolle. Gut durchgeführte und erfolgreiche Deals zeichnen sich durch Sorgfalt und Umsicht sowie wenige oder keine Probleme aus.

Doch oft sehen wir Fälle, bei denen ITDMs meinen, dass ihnen Zeit fehlt. Nur 36 % stimmen absolut zu, dass ihr IT-Team genug Zeit hat, um die IT-Sicherheitsstandards, -prozesse und -protokolle der Zielfirma zu überprüfen, bevor der Deal stattfindet. Obwohl die Prüfung der IT-Sicherheit mehr Aufwand und Zeit während des Prozesses erfordern kann, führt eine gründliche M&A-Analyse der IT-Sicherheitslage sehr wahrscheinlich zu einem besseren Gesamtergebnis und weniger Überraschungen.

ASSET-BEWERTUNG & INVENTARISIERUNG

Internen IT-Teams fehlen eventuell die Fähigkeiten für IT-Sicherheitsbewertungen:

37 %

Nur 37 % der ITDMs meinen, dass ihr IT-Team alle Fähigkeiten hat, um eine IT-Sicherheitsbewertung für die Akquisition durchzuführen.

US	UK	FR	DE	AUS	SG	IN
49 %	30 %	36 %	28 %	31 %	31 %	54 %

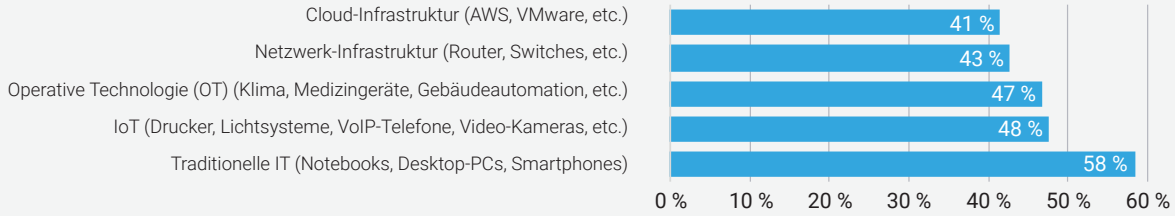
Geräte-Bewertung

Eine vollständige Asset-Inventarisierung ist unverzichtbarer Bestandteil einer soliden Abwehrstrategie. Die Fähigkeit, einen Überblick über das Netzwerk zu gewinnen, ermöglicht rechtzeitiges Reagieren und kann IT- und OT-Sicherheitsrisiken reduzieren. Wenn Unternehmen Assets betrachten, sollten sie alle potenziellen Schwachstellen ganzheitlich untersuchen. Doch trotz der notwendigen Asset-Erfassung und -bewertung zeigen die Antworten, dass die Teilnehmer die Bedeutung der Asset-Inventarisierung in den fünf Gerätekategorien Netzwerk, IoT, OT, traditionelle IT und Cloud-Infrastruktur unterschiedlich einschätzen.

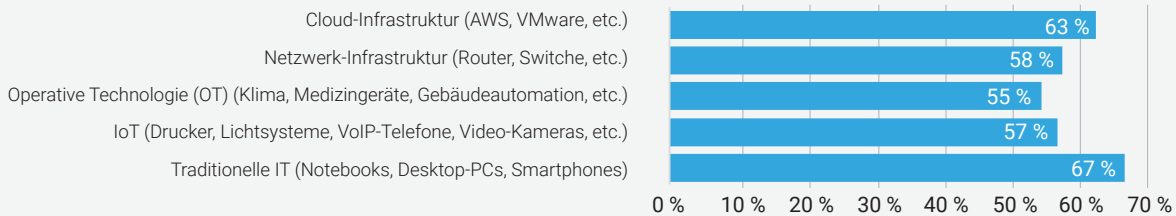
Die Umfrageergebnisse offenbaren die Lücke, wie viele der als besonders für externe Angreifer anfälligen Assets auch tatsächlich während der Akquisition bewertet werden. Ein Beispiel: 78 % der Befragten betrachten die Netzwerk-Infrastruktur (Router, Switches) als am anfälligsten für externe Angreifer; aber nur 58 % der ITDMs gaben an, dass die Netzwerk-Infrastruktur während der Akquisition bewertet wurde. Außerdem gaben 43 % der ITDMs an, dass die Netzwerk-Infrastruktur bei der Erfassung am ehesten übersehen wird.

Ebenso hielten 72 % der Befragten IoT-Geräte (wie Drucker, Lichtsysteme, VoIP-Telefone, Videokameras) für besonders anfällig für externe Angreifer; allerdings gaben nur 57 % der ITDMs an, dass IoT-Geräte im Rahmen der Akquisition bewertet wurden. 48 % der ITDMs meinten sogar an, dass IoT-Geräte bei der Geräteinventur am ehesten übersehen werden.

Welche Assets werden bei der Anlageninventur am ehesten übersehen?



Welche Assets beurteilt Ihr Unternehmen, um die Sicherheitslage bei der Integration einer Akquisition zu prüfen?



73 % der Befragten halten operative Technologie (OT) für am stärksten gefährdet; 55 % der ITDMs erklärten, dass die OT bewertet wurde. Aber 47 % gaben an, dass sie bei der Bestandsaufnahme übersehen wird. Diese Ergebnisse zeigen, dass, obwohl es erhebliche Bedenken hinsichtlich der Schwachstellen von Assets in der traditionellen IT-, OT-, IoT-, Cloud- und Netzwerk-Infrastruktur gibt, das Maß der Besorgnis nicht immer mit dem Grad der ergriffenen Maßnahmen übereinstimmt. Folglich gibt es auch erhebliche Sorgen, dass Assets und Geräte bei der Erfassung übersehen werden.

Diese Erkenntnisse machen klar, dass Business-Entscheider die Inventarisierung zwar als wichtigen Schritt der Bewertung ansehen, die Bestandsaufnahme aber oft ein schwieriges Unterfangen bei einer M&A bleibt.

Unterschiede in der Wahrnehmung bei Assets, die als am stärksten gefährdet gelten und wie oft sie tatsächlich bewertet werden:

78 %
Verwundbarkeit der Netzwerk-Infrastruktur

58 %
Bewertung der Netzwerk-Infrastruktur

43 %
Übergehen der Bewertung der Netzwerk-Infrastruktur

Geräte werden bei der Integration oft übersehen und nicht erfasst:

53 %

Mehr als die Hälfte der ITDMs sagen, dass Geräte nach Abschluss der Integration nicht erfasst waren.

US	UK	FR	DE	AUS	SG	IN
53 %	49 %	55 %	60 %	44 %	57 %	55 %

Warum Asset-Erfassung ein Kampf ist

Der Frage, ob dem eigenen IT-Team genügend Zeit für die Überprüfung von IT-Sicherheitsstandards, -Prozessen und -Protokollen der Zielfirma vor der Übernahme gegeben wurde, stimmten nur 36 % der ITDMs zu.

Auch der Frage, ob das eigene IT-Team fähig genug ist, die IT-Sicherheit für eine bestimmte Akquisition zu prüfen, bejahten nur 37 % der ITDMs.

Wichtige Entscheidungsträger sind nicht nur der Meinung, dass den eigenen IT-Teams oft die Zeit fehlt, um eine IT-Prüfung vor der Akquisition durchzuführen, sondern sie zweifeln auch an den Fähigkeiten ihrer IT-Teams. Angesichts dessen sollte man meinen, dass Unternehmen dazu neigen, in eine externe Evaluierung zu investieren. Allerdings gaben nur 57 % der ITDMs und BDMs an, dass ihr Unternehmen einen der größten vier Auditoren damit beauftragt.

Angesichts dessen verwundert es nicht, dass 80 % der ITDMs erklären, dass vorher unerkannte Cybersicherheitsprobleme immer erst bei der technischen Integration aufgedeckt werden.

Während diese Umfrage die Menge nicht erfasster Geräte nicht nach Kategorien aufschlüsselt, geben gut die Hälfte (53 %) der ITDMs an, dass Geräte am Ende der Integration nicht erfasst waren. Am häufigsten werden traditionelle IT-Geräte (Laptops, Desktops, Smartphones), und IoT- und OT-Geräte gefunden. Die Antworten zeigen aber auch, dass ein großer Teil der angeschlossenen Geräte vor der Akquise nicht erfasst wird. Klassische IT-Geräte sind oft am einfachsten zu finden und zu tracken. IoT- und OT-Geräte werden oft nicht erfasst, weil sie so klein sind (z.B. sind Sensoren kaum zu erkennen). Andere OT-Geräte laufen auf alter Hard- und Software wodurch sie schwieriger zu entdecken und patchen sind. Und manchmal fehlen Firmen schlicht die Werkzeuge, um jedes Gerät im Netzwerk zu identifizieren und komplett zu analysieren. Unabhängig von der Zahl nichterkannter Geräte, erbt ein Unternehmen ein Sicherheitsrisiko, wenn es auch nur ein Gerät übersieht – weil nicht klar ist, was man sich damit einfängt.

Viele Chancen der Kompromittierung

Durchschnittlich 43 % der Befragten gaben an, dass ihre Unternehmen bei der Inventarisierung einer Firma weniger als 10.000 angeschlossene Geräte finden. Größere Unternehmen analysieren noch mehr Geräte: 23 % der Befragten geben an, dass ihre Unternehmen über 500.000 Geräte finden. Das bedeutet, dass oft tausende Geräte als Teil einer Akquisition erworben werden, die gepatcht und sicher, oder gefährlich und voller Malware sein können. Und wenn man bedenkt, dass mehr als die Hälfte der ITDMs zusätzliche, nicht erfasste Geräte nach der Integration finden, sind die Chancen einer Infektion oder bösartiger Aktivitäten groß. Es braucht nur ein übles Gerät, um ein Netzwerk zu kompromittieren.

Die größten Risiko-Faktoren

Während der Studie haben wir gefragt, was das Unternehmen während der Informations- und Technologieintegration am meisten gefährdet. Drei Antworten stachen hervor: Konfigurations- und menschliche Fehler (51 %), vernetzte Geräte (50 %), sowie Daten- und Speichersysteme (49 %).

Der menschliche Faktor ist eine Herausforderung, die über M&A – als die Fehlerursache schlechthin hinausgeht: Als Insider-Bedrohung, unbeabsichtigtes Datenleck oder unerwünschter Malware-Download per Phishing-E-Mail. Um diese menschlichen Fehler zu reduzieren, nutzen viele Unternehmen Trainings-, Incentive- und Disziplinarprogramme.

VERZÖGERUNGEN & ENTTÄUSCHUNGEN

Das Unterschätzen der Cybersicherheit kann zu bösen Überraschungen führen:

65 %

Knapp zwei Drittel sagen, das ihre Unternehmen den Kauf einer Firma wegen IT-Sicherheitsmängeln bedauern.

US	UK	FR	DE	AUS	SG	IN
65 %	65 %	67 %	61 %	61 %	65 %	70 %

Zeitverzögerungen beim Zukauf

Zeitpläne, Ressourcen und Abläufe eines Unternehmens können sich insbesondere bei Fusionen und Übernahmen verändern. Knapp die Hälfte (49 %) der Befragten geben an, auf vorher unbekannte IT-Sicherheitsprobleme und -Risiken während der Integration von Daten und Technologien gestoßen zu sein, die die Integration verzögerten.

Diese Rückschläge können zu Verzögerungen oder Verlusten führen und das Unternehmen und seine M&A-Strategie negativ beeinflussen. Wir haben die Teilnehmer nach Verzögerungen von weniger oder mehr als 6 Monaten und Verlusten von weniger oder mehr als einer Mio. Dollar gefragt. Mehr als die Hälfte (54 %) nannten eine geringfügige Verzögerung (unter 6 Monaten) wegen eines Sicherheitsvorfalls, 50 % gaben mehr als 6 Monate an. Bei 22 % der Befragten lag der Verlust unter 1 Mio. Dollar, und nur 5 % hatten einen Verlust von mehr als 1 Mio. Dollar zu beklagen.

Mehrere Faktoren können zu diesen Verzögerungen und Kosten beitragen. Unternehmen können diese aber reduzieren, indem sie IT-Entscheider frühzeitig einbeziehen und ihnen für die Aufgaben nötigen Ressourcen bereitstellen. Tatsächlich sind 35 % der IT-Entscheider der Meinung, dass sie sich stärker in den M&A-Prozess in ihrem Unternehmen einbringen müssen.

Die Teilnehmer wurden nach Verzögerungen von weniger oder mehr als 6 Monaten und Verlusten von weniger oder mehr als 1 Mio. Dollar befragt.

54 %
geringe Verzögerung (<6 Monate)

50 %
größere Verzögerung (>6 Monate)

22 %
Verluste von weniger als 1 Mio. U$

5 %
Verluste von mehr als 1 Mio. U$

> Knapp die Hälfte (49 %) der Befragten geben an, auf vorher unbekannte IT-Sicherheitsprobleme und -Risiken während der Integration von Daten und Technologien gestoßen zu sein, die die Integration verzögerten.

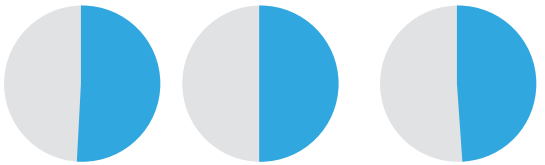
Akquisitions-Einbußen und -Probleme

Knapp zwei Drittel sagen, das ihre Unternehmen den Kauf einer Firma wegen IT-Sicherheitsmängeln bedauern.

21 % gaben an, dass ihr Unternehmen einen Kauf sehr bedauert, bei 44 % immerhin etwas, während 35 % der Befragten keine Einbußen beklagten.

Danach befragt, woher die Einbußen rühren, berichteten viele von Cyber-Vorfällen oder -Problemen. Die meisten Fälle bezogen sich auf eine schlechte Due Diligence oder Analyse, Zeit- und Geldverlust sowie Sicherheitsverstöße oder -angriffe. Bei der Frage, was sie hätten besser machen können, antworteten viele, sie hätten sich gewünscht, dass ihr Unternehmen einen Drittanbieter beauftragt hätte, um die IT-Sicherheit und das Unternehmen zu prüfen. Viele ergänzten den Wunsch, ihre Unternehmen hätten mehr Zeit oder weniger Geld in den Kauf oder die Transaktion gesteckt. Ein paar Beispiele:

Was gefährdet Unternehmen während der Daten- und Technologie-Integration am meisten:



51 %
menschliche Fehler und Konfigurations-Probleme

50 %
vernetzte Geräte

49 %
Daten- und Speicher-systeme

"Ich denke, mein Unternehmen wäre gerne proaktiver gewesen, was die Risiken der Cybersicherheit bei der Gründung unseres Unternehmens betrifft, und bedauert Vorfälle, die wegen laxer Regeln passiert sind. "

– Businessentscheider aus den USA

"Wir wünschten, wir wären mit unserer Due Diligence gründlicher gewesen." – UK-ITDM

"Wäre es möglich gewesen, hätte ich meinem IT-Team mehr Zeit für eine vollständige Inspektion gegeben." – IT-Entscheider aus Singapur

"Mein Unternehmen wünscht sich, dass es wasserdichte Verträge in Bezug auf Rückforderungen und Entschädigungen verhandelt hätte." –Australischer BDM

Cyber-Risiken besprechen

Generell waren die Antworten von ITDMs und BDMs in vielerlei Hinsicht ähnlich. So gab es große Übereinstimmungen bei ITDMs und BDMs, als es um die Einstufung der Cyber-Risiken in jeder Phase der Akquisition ging (Strategie, Zielsuche, Prüfung und Bewertung sowie Integration). ITDMs stuften die Integration am höchsten (7,52) ein – gegenüber BDMs (7,36).

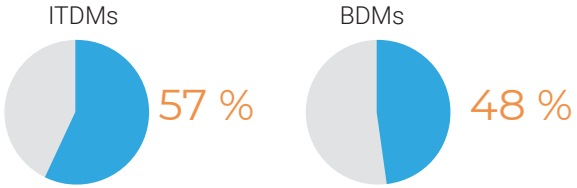
Es gab jedoch etliche Fälle, in denen sich die Meinungen, die Beteiligung oder der Ansatz zu einem bestimmten Thema unterschieden.

Zum Beispiel waren 51 % der ITDMs an der Integrations-Phase von M&A-Prozessen beteiligt, aber nur 35 % der BDMs. Man könnte eine höhere Beteiligung des ITDM an der IT-Integration erwarten, aber nicht unbedingt für die Integration als Ganzes.

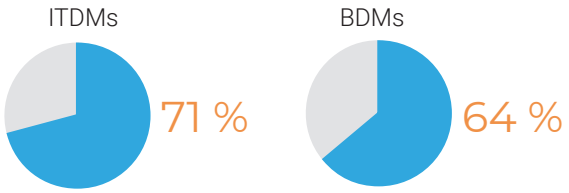
An der ersten Phase der Strategieentwicklung sind 73 % der ITDMs, aber nur 66 % der BDMs beteiligt. Die Daten zeigen, dass ITDMs in allen vier Phasen häufiger als BDMs involviert sind. Das deutet darauf hin, dass Unternehmen von einer stärkeren Beteiligung der BDMs profitieren würden.

Hier sind ein paar zusätzliche Vergleiche:

Die Teilnehmer gaben an, dass eine M&A-Transaktion ihres Unternehmens wegen eines kritisches IT-Sicherheitsproblems gefährdet war.



Die Bewertung der Cybersicherheit ist sehr wichtig.



Diese Antworten lassen auf zweierlei schließen:

Erstens, ITDMs und BDMs waren häufig, aber nicht immer einer Meinung. Selbst bei gleichen Ansichten zeigen ihre Antworten Verbesserungschancen im Bereich IT und Cyber-Risiken auf. So sollten sowohl ITDMs als auch BDMs in jeder Phase der Akquisition stärker einbezogen werden.

Zweitens suggerieren die Ergebnisse, dass ITDMs und BDMs Risiken unterschiedlich betrachten und priorisieren. Ein Beispiel: 23 % der ITDMs, aber nur 19 % der BDMs sagten, dass ihr Unternehmen nach einem M&A-Deal große Einbußen wegen IT-Problemen hinnehmen mussten. Diese wenn auch nur geringen Unterschiede zeigen, dass ITDMs und BDMs Risiken unterschiedlich quantifizieren können. Aus Sicht des ITDM ist der Absturz einer wichtigen Anwendung in der Integrationsphase sehr ärgerlich, weil Mitarbeiter und Kunden stundenlang nicht arbeiten können. BDMs betrachten ein solches Szenario eher unter dem Aspekt eines finanziellen Verlusts.

Vom ersten Tag einer Akquisition an müssen sich ITDMs und BDMs darüber einig sein, wie sie Risiken kommunizieren, berechnen, bewerten und reduzieren wollen. Da sie selten für dieselben Personen, Prozesse, Ressourcen und Aufgaben verantwortlich sind, können sie Risiken unterschiedlich angehen – mit verschiedenen Toleranzschwellen und verschiedenen Ansichten, wie die Folgen der Risiken zu kommunizieren sind. Damit alle Risiken sicher verstanden werden, müssen sich ITDMs und BDMs auf gemeinsame Begriffe und Maßnahmen der Risikobewertung und -kommunikation einigen.

FAZIT

Das Cyber-Sicherheitsrisiko ist ein zunehmendes Problem für IT- und Geschäftsentscheider beim Kauf und der Integration von Unternehmen. Während der Integration sind Unternehmen stärker Gefahren ausgesetzt und für Angriffe anfälliger, da sie nicht sehen können, was gefährdet und angreifbar ist. Zur Senkung dieser Risiken müssen IT-Teams frühzeitig sowohl die Zeit für eine intensive Bewertung, Prüfung und Inventur erhalten, als auch den Prozess vor Ort besser steuern können.

Unseren Umfrageergebnissen zufolge besteht für Unternehmen die Chance, ihre Wachsamkeit beim Schutz ihrer Unternehmen zu erhöhen, indem sie IT-Mitarbeiter schulen, IT-Teams stärker in den M&A-Prozess einbinden, ein automatisiertes Inventarisierungsprogramm für Assets einführen und ihnen die notwendige Zeit für die Durchführung der Due Diligence geben.

Die Ergebnisse dieses Berichts legen nahe, dass mehr Kontrollen zu deutlich besseren Ergebnissen führen, wenn es um die Risikobegrenzung und den Schutz der Unternehmens-Assets geht.

Mehr zur Minimierung von Cybersicherheitsrisiken erfahren Sie in unserem englischen **Solution Brief Mergers and Acquisitions**.

ÜBER FORESCOUT TECHNOLOGIES

Forescout Technologies ist führend in der Kategorie "Device Visibility and Control" (Gerätetransparenz und -kontrolle). Unsere einheitliche Sicherheitsplattform ermöglicht es Unternehmen und Behörden, ein vollständiges Lagebild großer Unternehmensnetze zu gewinnen und Maßnahmen zur Reduzierung von Cyber- und Betriebsrisiken zu orchestrieren. Forescout-Produkte sind dank agentenloser Echtzeit-Analyse sehr schnell einsetzbar. Sie klassifizieren und überprüfen kontinuierlich alle IP-Geräte Ihrer IT. Am 31. Dezember 2018 hatte Forescout 3.300 Kunden in über 80 Ländern, die sich auf infrastrukturunabhängige Lösungen von Forescout verlassen, um das Risiko von sicherheitsbedingten Ausfällen zu reduzieren, die Einhaltung von Sicherheitsrichtlinien sicherzustellen und nachzuweisen sowie die Effizienz der Sicherheitsprozesse zu steigern. Mehr dazu auf www.forescout.de.

Forescout-Forscher haben den Umfang und die Datenmengen aus Gründen der Konsistenz und des Handlings zur einmaligen Erstellung dieser Studie begrenzt. Wir haben die Einschränkungen aufgrund von Studienart und -zeit, Umfang, Daten-Anonymisierung, passiven Erfassungsmethoden und Fehlern bei KI-basierter Klassifizierung von Gerätefunktionen, Betriebssystemen und Anbietern festgelegt. Die Nutzung realer Cloud- und Steuerungssystemdaten in Echtzeit kann zu Ungenauigkeiten in der Datenerfassung führen. Innerhalb dieser Grenzen haben die Forescout-Forscher ihr Bestes getan, um eine konsistente, zuverlässige und stimmige Studie zu erstellen.

EMPFEHLUNGEN

Firmenkäufe können zeit- und ressourcenintensiv sein, und manchmal lassen sie sich aufgrund von Erkenntnissen aus der Due Diligence leider nur abbrechen. Früher konzentrierten sich die Bewertungen vor allem auf Finanzen, Recht, Vertrieb, Produktion, Personal und IT. Und obwohl IT-Sicherheit als eigener Bewertungsbereich nicht völlig ignoriert wurde, ist klar, dass Unternehmen mit Kaufabsichten angesichts der Risiken von einer umfassenden und gezielten Cyber-Evaluierung profitieren können. Nachfolgend finden Sie einige Empfehlungen für Unternehmen, die sich auf ihren nächsten Geschäftsabschluss vorbereiten.

Früh investiertes Geld wird sich als gut angelegt erweisen, wenn es Sie auf Ihrem Weg vor Überraschungen schützt.

Auf Asset-Management und -Inventarisierung fokussieren: Wenn Unternehmen es versäumen, Geräte und Anlagen in ihrem Netzwerk zu erfassen, fehlt das Wissen, welche Risiken sie bei der Akquisition mit einkaufen. Asset-Management und -Inventarisierung sind für Unternehmen der beste Weg und sehr wichtig, um Sicherheitsrisiken bei M&A zu reduzieren. Und im nächsten Schritt muss die relative Bedeutung jedes Assets ermittelt und ein tiefes Verständnis des mit ihm verbundenen Netzwerks gewonnen werden. Anders gesagt: Wenn sich ein gefährdetes Objekt im Netzwerk befindet, das aber segmentiert ist, lassen sich das Objekt und dessen Risiko dennoch effektiv verwalten.

Ermöglichen Sie internen Teams, gründliche Prüfungen durchzuführen und externe Hilfe hinzuzuziehen (wenn dem Team für die Due Diligence wichtigen Fähigkeiten fehlen). Unternehmen müssen einsehen, dass sie eventuell nicht immer alles selbst schaffen können, und dass interne Teams für eine umfassende Due Diligence wichtige Schulungen benötigen.

Reservieren Sie Budgets für externe Sicherheits-Audits: Seien Sie bereit, das erforderliche Geld auszugeben, damit Ihr Unternehmen eine gründliche Prüfung vor Abschluss des Deals durchführt. Früh investiertes Geld wird sich als gut angelegt erweisen, wenn es Sie auf Ihrem Weg vor Überraschungen schützt.

Schulen Sie Ihre IT-Teams, damit sie für die Vorbereitung und Abwicklung einer Akquisition bestens gerüstet sind: IT-Teams benötigen auch Schulungen, um zu wissen, wonach sie suchen und wie sie mit M&A-Problemen umgehen sollen. Unterhändler können sich auch mit Systemen und Protokollen über Sicherheitsprobleme informieren, aber sie müssen über neueste Angriffe direkt informiert werden.

Intensivieren Sie Kontrollen, um Ihr Unternehmen zu schützen: Unternehmen mit fortschrittlichen IT-Sicherheitskontrollen identifizieren, verstehen, verwalten und mindern M&A-Risiken besser.

Berücksichtigen Sie Eventualitäten und Rückforderungen: Obwohl 89 % der Befragten meinen, dass ihr Unternehmen Rückforderungen vorsehen sollte, tun es derzeit nur 69 %. Rückforderungsklauseln sind ein gängiger Weg, um Risiken zu mindern, falls plötzlich Probleme oder Wertverluste auftauchen. Rückfallklauseln nutzen 73 % der Befragten, um ein Geschäft nach der Unterzeichnung zu canceln, wenn sich Zusicherungen und Gewährleistungen als nicht haltbar erweisen.

Erfahren Sie mehr auf Forescout.de

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

E-Mail: info-dach@forescout.com
Tel (Intl): +1-408-213-3191
Support: +1-708-237-6591