Whitepaper

Bitdefender®

Die Rolle des CIO wächst mit der Virtualisierung

(Eine Studie unter IT-Entscheidern in Deutschland)

Zusammenfassung:

Die Studie von Bitdefender unter 100 IT-Entscheidern in deutschen Unternehmen mit mehr als 1000 PCs im Einsatz zeigt, dass die Rolle der IT innerhalb der Unternehmenshierarchien zunehmend wichtig wird. CEOs und Vorstandsmitglieder sind einer wachsenden Zahl interner und externer Sicherheitsrisiken ausgesetzt, die das Potenzial haben, Kundenvertrauen und Geschäftserfolg nachhaltig zu beinträchtigen. Dennoch haben nicht alle Vorstandsetagen bereits einen CIO oder CISO in ihren Entscheidungsprozessen eingebunden. Die von iSense Solution durchgeführte Studie zeigt auf, wie Entscheidungsträger in der IT ihre Rolle innerhalb von Organisationen wahrnehmen und was sie benötigen, um die Erwartungen des Unternehmens an sie zu erfüllen. Wie hat das Thema Virtualisierung die Spielregeln für Security verändert? Können Angriffe mit den gegebenen Mitteln gestoppt werden? Sind Unternehmen zu Zahlungen bereit, wenn Sie damit eine öffentliche Bloßstellung vermeiden können?

Wichtigste Erkenntnisse der Studie:

- Mehr als ein Drittel aller CIOs gaben an, dass ihre Tätigkeit innerhalb der Unternehmenshierarchie an Bedeutung gewonnen hat. Ein Zehntel aller Befragten gab sogar an, dass sich ihre Tätigkeit sich in den vergangenen Jahren komplett verändert hat.
- Sieben von zehn IT-Entscheidern gaben an, das Thema IT-Sicherheit habe oberste Priorität für ihr Unternehmen. Allerdings stimmen weniger als die Hälfte mit der Aussage überein, ihr Budget für IT-Sicherheit sei ausreichend. Die Ausgaben für Cloud-Security wuchsen innerhalb eines Jahres um 36 Prozent an, während die IT-Sicherheitsausgaben für andere Bereiche gleichblieben.
- Dabei haben die Ausgaben für Cloud-Security fast das Ausmaß für physikalische Security erreicht.
- Mehr als ein Viertel aller Cyberangriffe können mit gegebenen Mitteln nicht gestoppt, erkannt oder verhindert werden.
- Rund 12 Prozent aller befragten Unternehmen haben in den vergangenen zwölf Monaten eine Sicherheitspanne erlebt. 83 Prozent aller IT-Entscheider wissen nicht, was die Ursache hierfür war.
- Mehr als die Hälfte der befragten Unternehmen in Deutschland sind dazu bereit, im Schnitt 80.000 Euro zu bezahlen, wenn dadurch ein öffentlicher Skandal und damit verbundene Bloßstellung des Unternehmens vermieden werden könnte. Rund sechs Prozent sind sogar dazu bereit hierfür mehr als 500.000 Euro zu bezahlen.

Im Jahr 2016 war vor allem ein Anstieg von bislang unbekannten Sicherheitsbedrohungen zu verzeichnen. IT-Entscheider stehen somit vor der Herausforderung, neue Technologien einzusetzen, mit denen Zero Day Exploits, Advanced Persistant Threats (APTs) und andere Arten von Cybercrime bekämpft werden können. Zudem haben Virtualisierung und der Einsatz hybrider Umgebungen zu einer signifikanten Vergrößerung der Angriffsoberfläche geführt, was den Entscheidungsträgern erhebliche Kopfschmerzen bereitet, da sie für die komplette Infrastruktur verantwortlich sind , egal ob physisch oder virtuell. Immer mehr Unternehmen vertrauen sensible Daten und Arbeitsprozesse ihren Cloud Providern an. Bereits 63 Prozent der Unternehmen haben IT-Prozesse in die Cloud verlagert, 36 Prozent Geschäftsprozesse, 34 Prozent Customer Support, Marketing und Sales und 32 Prozent haben sogar schon Finanzprozesse in die Cloud verlagert.[1].

Der Markt für hybride Cloud-Lösungen wird gemäß einer Studie von MarketsandMarkets bis 2019 jährlich um 27 Prozent wachsen.[2] Das Marktforschungsunternehmen erwartet, dass der Markt für hybride Cloud-Lösungen sich von 2014 und $25 Milliarden US-Dollar bis zum Jahr 2019 auf $85 Milliarden US-Dollar mehr als verdreifachen wird. Bei einer Befragung im Rahmen einer Tech-Konferenz von Gartner

1 "Moving forward with cybersecurity and privacy", PwC, Oct 2016, http://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf

2 SPECIAL REPORT: CIOs Say Hybrid Cloud Takes Off, WSJ, http://blogs.wsj.com/cio/2015/10/20/special-report-cios-say-hybrid-cloud-takes-off/

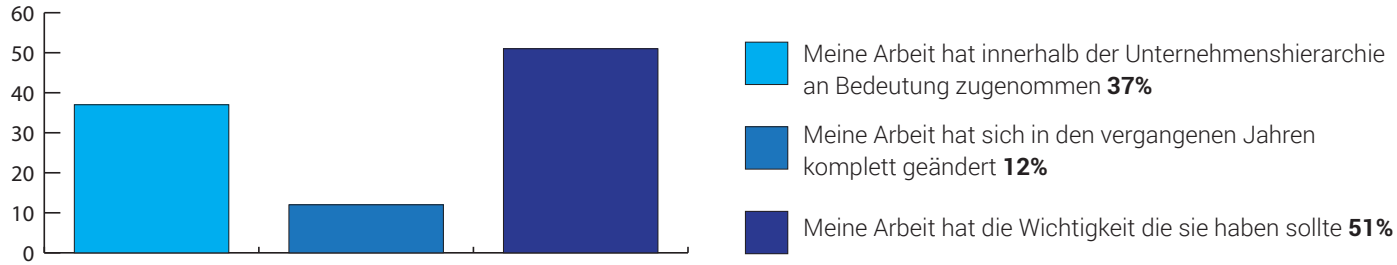
gaben 75 Prozent der Großunternehmen an, bis zum Ende des vergangenen Jahres, hybride IT-Installationen durchgeführt zu haben. Große Unternehmen, die bereits massiv in On-Premises-Architekturen investiert haben und ihre Daten dennoch in die Cloud migrieren, werden zu den größten Botschaftern für das hybride Modell entwickeln.

Dieser Wandel vollzieht sich zu einer Zeit, in der Ransomware-Angriffe immer häufiger vorkommen. Die finanziellen Verluste durch Ransomware im Jahr 2016 alleine werden von Experten auf gut eine Milliarde Dollar geschätzt und stellen für Cyberkriminelle damit eine sehr profitable Einnahmequelle dar. Die Angriffe, die darauf ausgerichtet sind, über APTs geistiges Eigentum und Kundendaten auszuspionieren und schnelles Geld zu machen, sind bisher sehr erfolgreich, womit sich die HYPERLINK "http://businessinsights.bitdefender.com/predictions-for-2016" Vorhersagen zur Bedrohungslandschaft für 2016 von Bitdefender bewahrheitet haben.

„Auf Unternehmensseite werden wir einen Anstieg von zielgerichteten Angriffen und vernebelnden Bots mit kurzer Lebenssauer und häufigen Updates beobachten. Die meisten dieser Angriffe werden sich auf Informationsdiebstahl spezialisieren", sagte Bogdan Dumitru, Chief Technology Officer bei Bitdefender bereits im Dezember 2015. „Angreifer werden in wenigen Tagen, vielleicht sogar in wenigen Stunden in Organisationen eindringen und wieder draußen sein. APT, das für Advanced Persistant Threats steht, sollte in „BA" für Blitzkrieg-Angriffe umbenannt werden. Quer-Bewegungen in die Infrastruktur von Cloud-Dienstleistern werden häufiger zu beobachten sein und damit einhergehend werden auch neue Tools verfügbar sein, die es Angreifer ermöglichen, den Hypervisor einer virtuellen Instanz zu kompromittieren und zwischen unterschiedlichen virtuellen Maschinen zu springen. Das Szenario ist besonders gefährlich für sogenannte „Bad Neigbourhood"-Umgebungen, bei denen eine böswillige Partei Zugriff auf ein physisches System über einen seriösen Dienstleister oder Unternehmen erhalten kann."

Eine Studie von Bitdefender unter deutschen Großunternehmen hat jetzt herausgefunden, dass der ***wachsende Druck durch Sicherheitsvorfälle und Blitzkrieg-Angriffe*** CEOs dazu gebracht hat, CIOs als die wichtigsten C-Level Manager anzusehen die gemeinsam mit COOs und CFOs entscheidende strategische Entscheidungen treffen und das Thema Sicherheit fest auf Vorstandsebene verankern. Rund 37 Prozent der IT-Entscheider geben an, dass ihre Tätigkeit innerhalb der Unternehmenshierachie an Bedeutung gewonnen hat. Währen 30 Prozent angeben, Ihre Tätigkeit habe sich in den vergangenen Jahren komplett verändert.

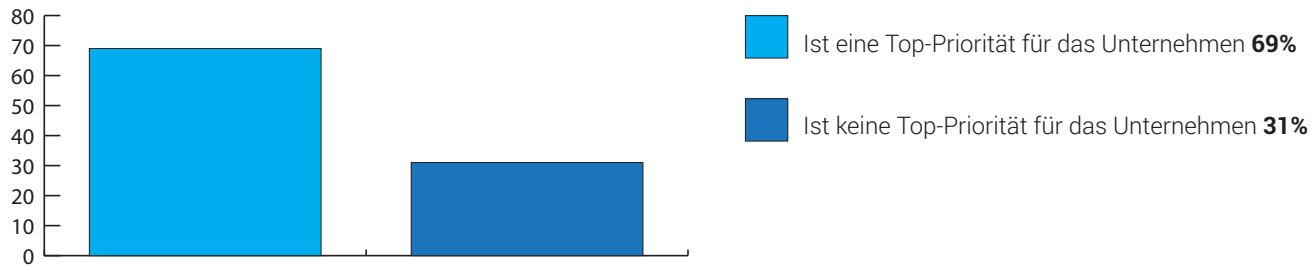
Hybride Umgebungen brachten die CIOs in die Vorstandsetagen (%)



Obwohl 7 von 10 IT-Entscheider das Thema IT Sicherheit als Top-Priorität für ihre Unternehmen ansehen, gehen sie davon aus, dass die Budgets um 8 Prozent erhöht werden müssten, um effiziente Sicherheitsmaßnahmen ergreifen zu können.

Die mangelnde Interaktion mit den Managementetagen gehört laut Gartner zu den wesentlichen Gründen für divergierende Risikoeinschätzungen von Sicherheitsverantwortlichen und Managementebene. Dies kann zu sich wiederholenden und falsch durchgeführten Kontrollen führen, die in unnötigen Auditierungen und letztlich zu einer reduzierten Produktivität führen. [3].

Sichtweise auf IT-Sicherheitsbudgets (%)



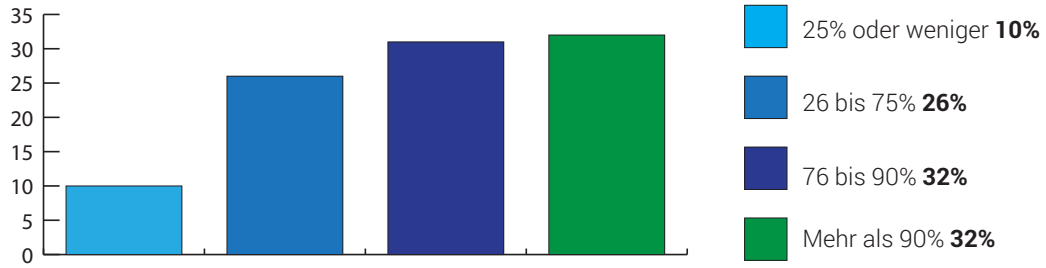
3 "Gartner Survey Shows Information Security Governance Practices Are Maturing", Gartner, July 21, 2015, http://www.gartner.com/newsroom/id/3098118

Die Studie von Bitdefender zeigt auf, dass 48 Prozent der IT-Entscheider denken, dass das Budget für IT-Sicherheit nicht ausreicht, 36 Prozent geben an, dass das Budget ausreicht, aber das Personal nicht ausreicht und 13 Prozent geben an, dass Budget sei ausreichend, aber nicht in Einklang mit künftigen Expansionen. Nur drei Prozent sagen, das Budget für IT-Sicherheit sei ausreichend.

Dass das Thema IT-Sicherheit auf Vorstandsebene angekommen ist, wird von einem von drei CEOs bestätigt, die angeben, dass sie sich fünf bis sechsmal in den vergangenen zwölf Monaten auf Vorstandsebene getroffen haben um über das Thema Cyber-Security zu sprechen. Diese Entwicklung wird weiter voranschreiten, da die Ausgaben für IT-Sicherheit weiter steigen werden und immer mehr CIOs davon ausgehen, dass Hacker in den kommenden zwei bis fünf Jahren die Oberhand gewinnen könnten. Daher sind stärkere und innovativere Verteidigungsmaßnahmen erforderlich – das haben auch viele CEOs inzwischen verstanden. Problematisch ist weiterhin, dass CIOs nicht sämtliche Angriffsmethoden der Hacker kennen, mit denen sie Systeme infiltrieren und Unternehmen ihre Sicherheitsmaßnahmen nicht offenlegen möchten – wie vergangene Studien bestätigt haben. [4].

Wie die Bitdefender-Studie zeigt, sind die Ausgaben für Cloud Security bei den befragten Unternehmen im vergangenem Jahr um 36 Prozent gestiegen, während die IT Security-Budgets für andere Sicherheitsmaßnahmen gleich geblieben sind. Fast die Hälfte der befragten Entscheidungsträger sagt zudem, dass Sicherheitsbudget sei ausreichend, während der Rest durchschnittlich einen Budgetanstieg um acht Prozent benötigt um effiziente Sicherheitsmaßnahmen bereitstellen zu können. Die Erklärung hierfür liegt hauptsächlich darin, dass die Migration von Informationen von herkömmlichen Rechenzentren in eine Cloud-Infrastruktur die angreifbare Oberfläche eines Unternehmens signifikant vergrößert hat und dadurch neue Bedrohungen und Sorgen hinsichtlich der Sicherheit der Daten für den CIO entstehen. Die Gesamtheit der befragten IT-Entscheidungsträger gab im Durschnitt an, dass mit gegebenen Ressourcen, lediglich 74 Prozent aller Cyber-Angriffe gestoppt, erkannt oder verhindert werden können.

Angriffe die mit aktuellen Ressourcen gestoppt/erkannt/verhindert werden können (%)



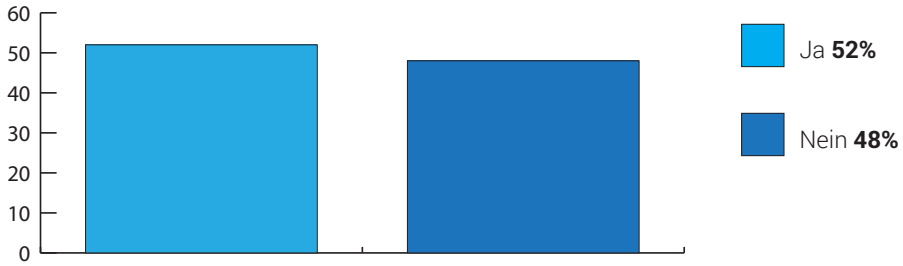
Die Studie zeigt, dass 12 Prozent aller Unternehmen in den vergangenen 12 Monaten eine Sicherheitspanne zu verzeichnen hatten, und 83 Prozent der Entscheidungsträger nicht wissen, was hierfür die Ursache war.

Cyberkriminelle können viel Zeit innerhalb einer Organisation verbringen, ohne dabei entdeckt zu werden, denn APTs werden oftmals so konzipiert, dass sie nicht erkannt werden. Gemäß des Paradigmas der Virtualisierung, wonach Aktivitäten im Raw Memory nicht verschlüsselt sondern lediglich zerhackt werden, können APTs versuchen, auf einer virtuellen Maschine Schadcode auszuführen. Dies kann nur durch Lösungen wie Bitdefenders Hypervisor Introspection Technologie (HVI) unterbunden werden bevor das Betriebssystem kompromittiert wird. Sobald der Schadcodes im Arbeitsspeicher der VM ausgeführt wird, selbst wenn er über einen Zero Day Exploit kam, kann die Intrusion Inspection Engine die bösartige Aktion und den Code, der ausgeführt werden soll, sofort erkennen.

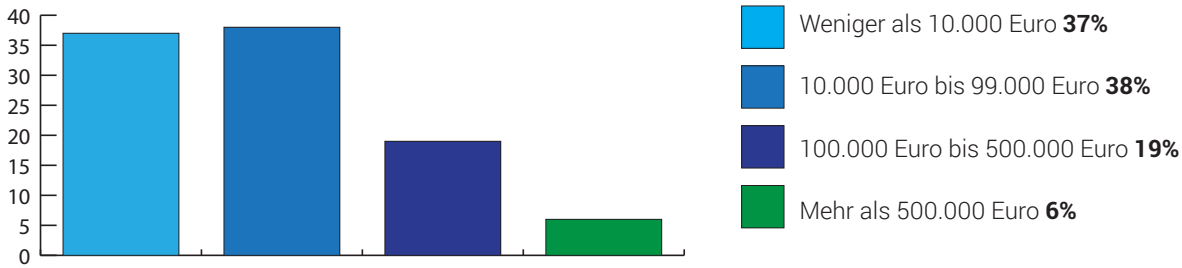
Mehr als die Hälfte aller Befragten Unternehmen in Deutschland sind bereit, durchschnittlich 71.000 Euro zu bezahlen, um einen öffentlichen Skandal und eine Bloßstellung zu vermeiden, die mit einem Sicherheitsvorfall einhergehen. Fast sechs Prozent sind sogar dazu bereit, mehr als 500.000 Euro zu zahlen und bestätigen damit indirekt, dass negative Schlagzeilen substantielle finanzielle Konsequenzen nach sich ziehen können. In einem aktuellen Fall haben Vertreter von Verizon, einem der größten Telekommunikationsanbieter in den USA und seit kurzem wichtigster Eigentümer von Yahoo, öffentlich erklärt, dass der letzte große Sicherheitsvorfall bei Yahoo, der zu einem der größten jemals stattgefundenen gehört, einen bedeutsamen finanziellen Einfluss auf die Verhandlungen mit Yahoo hatte. Das ist ein weiterer Beleg dafür, dass Cyber-Vorfälle dazu in der Lage sind, signifikante Transaktionen aufgrund des Drucks durch Anteilseigner und Medien zu unterbinden. In den Köpfen der Vorstandsmitglieder sollten IT-Entscheidungsträger in C-Level-Anzügen für Vorfälle geradestehen müssen. Gibt es Probleme beim schnellen und effizienten Agieren im Falle eines Sicherheitsvorfalls, kann das CIOs und IT-Manager den Job kosten.

4 "The Defender's Dilemma Charting a Course Toward Cybersecurity", http://www.rand.org/pubs/research_reports/RR1024.html

Zahlungsbereitschaft zur Vermeidung eines Sicherheitsvorfalls (%)



Betrag, den Unternehmen bereit sind zu zahlen (%)



Mit diesen Ergebnissen im Hinterkopf, sollten Organisationen, die im Begriff sind eine hybride Cloud-Lösung zu erwerben, einige praktische Hinweise berücksichtigen, um sicherzustellen, dass ihre Daten und die Daten ihrer Kunden jederzeit geschützt sind.

1. Definieren Sie die Kriterien, die beschreiben, welche Daten Sie On-Premises und welche sie in der Cloud speichern. Betreiben Sie Risikomanagement.

Sicherheitsspezialisten empfehlen, dass Unternehmen die über eine hybride Cloud-Lösung nachdenken, zunächst die Daten mit denen sie zu tun haben, analysieren und deren Sensibilität evaluieren sollen, und zwar sowohl für das Unternehmens als auch für den Kunden. Kritische, persönliche und private Daten, die in Bezug zu geistigem Eigentum stehen, müssen On-Premises gesichert werden, mit Zugang nur für autorisierte Mitarbeiter.

2. Halten Sie die Cloud privat

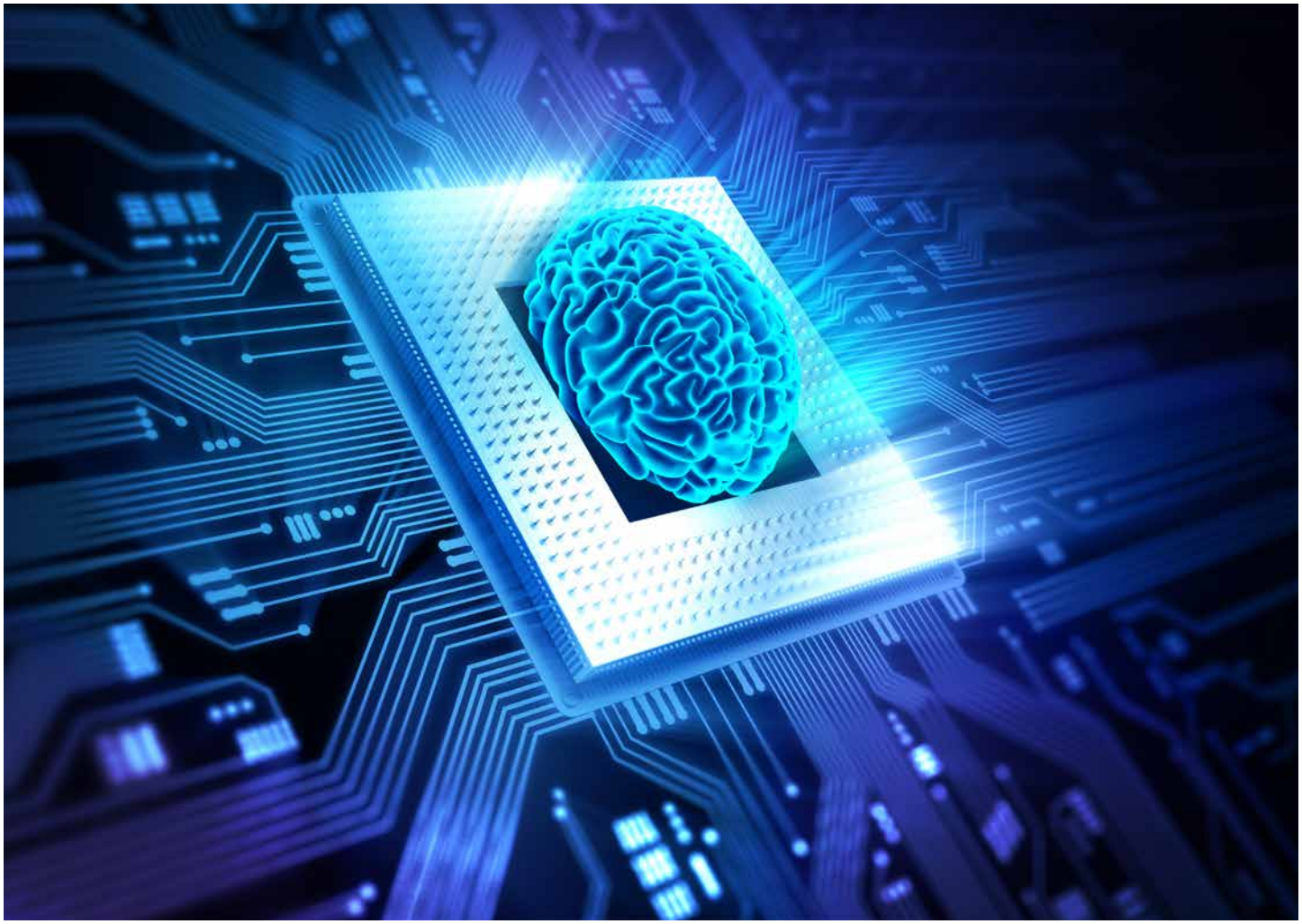
Organisationen die mit sensiblen oder vertraulichen Daten agieren oder mit Daten, die mit geistigem Eigentum zusammenhängen, müssen sicherstellen, dass die Private-Cloud-Infrastruktur privat bleibt. Niemand außerhalb des lokalen Netzwerks sollte in der Lage sein, auf Daten zuzugreifen und nur autorisiertes Personal sollte mit diesen Daten umgehen dürfen. Die Private Cloud muss vom öffentlichen Internetzugriff komplett isoliert sein um zu verhindern, dass Angreifer über Fernzugriff Schwachstellen ausnutzen und auf Daten zugreifen

3. Berücksichtigen Sie lokales Recht und Gesetze zur Datenspeicherung

Wenn Sie einen Cloud-Dienstleister auswählen ist es sehr wichtig, dass das Rechenzentrum in einer Region oder einem Land seinen physischen Sitz hat, in denen die Gesetze zur Datenhandhabung und -sicherung im Sinne der Geschäftsinteressen Ihres Unternehmens ausfallen. Jedes Rechenzentrum, unabhängig welche Daten dort gesichert sind, agiert unter den Datenschutzgesetzen des jeweiligen Landes, in denen das Rechenzentrum steht. In der Konsequenz müssen Unternehmen, die einen Cloud-Dienstleister außerhalb ihres Landes in Betracht ziehen, sehr genau die lokalen Datenschutzgesetze überprüfen. Ansonsten riskiert die Organisation rechtliche Konsequenzen, die finanzielle Schäden und eine Beschädigung der Reputation nach sich ziehen können.

4. Überprüfen sie ihren zukünftigen Cloud-Dienstleister mit hoher Sorgfalt

Wenn Sie einen Cloud-Dienstleister auswählen, ist ein „Due Diligence"-Überprüfung unerlässlich. Dabei müssen nicht nur die Fähigkeiten des Dienstleisters hinsichtlich ihrer Anforderungen überprüft werden, sondern auch seine Fähigkeit, im Falle eines technischen Unfalls (z.B. bei Stromausfällen, Beschädigung von Daten, Hardware-Fehler) oder bei Naturkatastrophen (z.B. Erdbeben, Brandkatastrophen) den Schaden beheben zu können. Mit diesen Fähigkeiten können Sie Ihre Geschäftsprozesse aufrecht halten und es hilft Ihnen dabei, Notfallprozeduren zu erstellen und durchzusetzen. Diese müssen vorhanden sein, um einen Unfall jeglicher Art ohne schwerwiegende Folgen zu überstehen.



[6]

5. Verschlüsseln Sie Daten – lokal und bei der Übertragung
Security-Spezialisten von Bitdefender empfehlen, dass jede Datenübertragung zwischen Kunde und Cloud-Dienstleister verschlüsselt sein sollte. Damit lassen sich Man-In-The-Middle-Angriffe vermeiden, mit denen übermittelte Daten abgefangen und entschlüsselt werden könnten. Darüber hinaus, sollten lokal oder in der Cloud gespeicherte Daten immer verschlüsselt sein um sicherzustellen, dass Cyberkriminelle sie im Falle einer Datenpanne oder durch unerlaubten Zugriff, nicht lesen können.

6. Sichern Sie die Daten in der Cloud
Um die Geschäftsprozesse aufrechtzuerhalten sollten Organisationen Backup- und Recovery-Mechanismen im Einsatz haben. Bevorzugter Weise sollten die Sicherung in standort-fernen, physischen und virtuellen Standorten stattfinden, die sich von denen Ihres Cloud-Dienstleisters unterscheiden. Damit minimieren Sie die Risiken durch menschliche Fehler oder Naturkatastrophen.

7. Verwenden Sie sichere und multiple Authentifizierungs-Mechanismen
Der Zugriff auf jedwede Art von Daten, in der Private oder Public Cloud, muss über multiple Authentifizierungs-Mechanismen erfolgen. Diese sollten mehr umfassen als lediglich Benutzernamen und Passwörter. Für den Zugriff auf kritische Daten bieten eine Zwei-Faktor-Authentifizierung , oder sogar eine biometrische Überprüfung, zusätzliche Kontrolle und Autorisierung der qualifizierten Mitarbeiter.

8. Nur eine begrenzte Anzahl an Mitarbeitern sollten Zugriff auf sensible Daten haben
Auschließlich autorisiertes Personal benötigt Zugriff auf wichtige und sensible Daten und nur bei Einhaltung eines strikten Security-Protokolls und moderner Authentisierungsmechanismen. Neben einer Zwei-Faktor-Authentisierung kann sogar eine Zwei-Personen-Authentisierung für besonders kritische Systeme eingesetzt werden - ähnlich wie bei Unternehmen im Finanzwesen, wo große Transaktionen von zwei odere mehreren Individuen authorisiert werden muss.

9. Beugen Sie DDoS-Angriffen vor
Distributed Denial of Service (DDoS)-Angriffe können Cloud-Dienste einschränken oder gar komplett zum Erliegen bringen. Daher müssen Organisationen Systeme einsetzen, die in der Lage sind, DDoS-Angriffen automatisch zu begegnen um die Aufrechterhaltung der Geschäftsprozesse sicherzustellen – und das sogar wenn solche Angriffe gerade stattfinden. Das Kontinuierliche Beobachten des Netzwerk-Traffics um Anomalien und Ungereimtheiten zu identifizieren ist ebenfalls sinnvoll.

10. Erstellen, definieren und implementieren Sie schnell greifende Security-Response-Prozesse
Unternehmen müsse eine Reihe von Prozessen und Richtlinien definieren, an denen sich sämtliche Stakeholder halten, um Sicherheitsvorfällen richtig begegnen zu können. Diese müssen Technologien und Methoden zur Identifikation, Isolation und Bereinigung von Sicherheitsvorfällen abdecken. Nach jedem Sicherheitsvorfall ist es unbedingt erforderlich, dass die Auswirkungen auf Unternehmen und Infrastruktur evaluiert werden, um anschließend neue und notwendige Sicherheitsmechanismen einzuführen, mit denen ebensolche Arten von Sicherheitslücken oder Schwachstellen nicht mehr ausgenutzt werden können.

Methodik

Im Auftrag von Bitdefender wurde diese Studie im Oktober 2016 von iSense Solutions durchgeführt. Dazu wurden 100 IT Profis (CIOs, CEOs, CISOs – 27 Prozent; IT Manager und Direktoren – 39 Prozent; IT System Administratoren – 25 Prozent, IT Support-Spezialisten – 5 Prozent und andere) in deutschen Unternehmen mit 1.000 oder mehr Computerarbeitsplätzen befragt.

Mehr als 40 Prozent der befragten Unternehmen kommen aus der IT Hardware- und Software-, Elektronik- und Elektroingenieurs-Industrie, 20 Prozent kommen aus dem produzierendem Gewerbe, 16 Prozent aus Transport & Logistik, 10 Prozent sind Anbieter von Telekommunikationsdiensten und der Rest kommt aus den Bereichen Bau, Handel, Medien oder anderen Branchen.

Rund 49 Prozent der befragten Unternehmen haben über 3.000 Mitarbeiter, 6 Prozent haben zwischen 2.000 und 2.999 Mitarbeiter und 45 Prozent haben zwischen 1.000 und 1.999 Mitarbeiter.

In Bezug zur IT Infrastruktur der befragten Unternehmen verfügen 29 Prozent über mehr als 3.000 Computer, 19 Prozent verfügen zwischen 2.000 und 2.9999 und 52 Prozent zwischen 1.000 und 1.999 Computer. Der durchschnittliche Anteil der Mitarbeiter, die an einem Computer arbeiten, beträgt 70 Prozent.

Autor: Răzvan Mureșan

Bitdefender ist ein globales Sicherheits-Technologie-Unternehmen und bietet wegweisende End-to-End Cyber-Security-Lösungen sowie Advanced Threat Protection für über 500 Millionen Nutzer in mehr als 150 Ländern. Seit 2001 ist Bitdefender ein innovativer Wegbereiter der Branche, indem es vielfach ausgezeichnete Schutzlösungen für Privat- und Geschäftsanwender einführt und entwickelt. Das Unternehmen bietet Lösungen für die Sicherheit hybrider Infrastrukturen als auch für den Schutz von Endpunkten. Als führendes Security-Unternehmen pflegt Bitdefender eine Reihe von Allianzen sowie Partnerschaften und betreibt eine umfassende Forschung & Entwicklung. Weitere Informationen sind unter www.bitdefender.de verfügbar..

BD-Business-Feb.20.2017-TK#: 70585