Weiterstadt, 08. Juni 2020

Ergebnisse zu der Devoteam-Umfrage CYBERSECURITY: Wie kann man die unterschiedlichen Interessen in Unternehmen zum Thema Cyber-Security erfolgreich kanalisieren und beherrschen?

Weiterstadt, 08. Juni 2020 - Devoteam (Euronext Paris: DVT), der führende IT-Dienstleister und Pure Player in der Digitalen Transformation in EMEA, hat gemeinsam mit IDC eine Umfrage zum Thema Cyber-Security „A Plan for Security Transformation" durchgeführt und die Ergebnisse veröffentlicht. Die drei Schwerpunktthemen der Umfrage werden von Devoteam auch in Form von Whitepapers bereitgestellt. Die Umfrage zeigt, dass die Business-, Security- und IT-Entscheider in den Unternehmen noch immer unterschiedliche Prioritäten hinsichtlich der Umsetzung von Cyber-Security haben. Teilweise wird auch die Sicherheit von Informationssystemen und Netzen noch als Einschränkung des Kerngeschäftes wahrgenommen.

Wichtigste Erkenntnisse aus der Umfrage:

- **Die funktionalen Entscheidungsträger haben unterschiedliche Prioritäten beim Thema Verbesserung der Cyber-Security im Unternehmen.**

  Die befragten Stakeholder-Gruppen orientieren sich an den Hauptzielen einer Digitalen Transformation, wie Innovation, Kreation von Produkten/ Dienstleistungen und Beschleunigung bei der Markteinführung. Die funktionalen Entscheider haben dabei jeweils eigene Prioritäten. Nach der Umfrage erwarten 58,28% der Business Manager von der Security Transformation eine Verbesserung des Engagements der Geschäfts-bereiche. Für 61,97% der IT-Verantwortlichen ist die Systemintegration das

übergeordnete Ziel, während für die Security-Verantwortlichen vor allem die Informationssicherheit (65,28%) im Vordergrund steht. Derartige konkurrierende Prioritäten sind nicht förderlich für eine erfolgreiche Transformation der Geschäftsabwicklung durch die Digitalisierung.

Die Einhaltung der Rechtsvorschriften und die Neuausrichtung der Unternehmen hin zu digitalen Vertriebskanälen gehören ebenfalls zu den Prioritäten, diese wurden von den Befragten an die zweite bzw. dritte Stelle ihrer Prioritätenliste gesetzt.

- **Die Komplexität des Themas Cyber-Security macht es für Unternehmen schwierig, die richtigen Ansatzpunkte zu finden.**

  Budget-Zwänge behindern die Verbesserung der Informationssicherheit in Unternehmen und Organisationen. Bei der Auswertung der Umfrage über alle Entscheider-Profile hinweg kam es zu folgendem Bild: 47,09% aller Befragten sehen das Budget, vor dem Fachkräftemangel (40,93%) und der Fragmentierung bzw. der mangelnden Integration des Produktportfolios von Sicherheitsprodukten (39,93%) als größte Herausforderung.

  Im Einzelnen positionieren die Business Manager an erster Stelle der Herausforderungen die Budget-Zwänge (52,98%), gefolgt von Qualifikationsdefiziten (43,71%) und den Schwierigkeiten die Sicherheits- mit Unternehmens- und Produktivitätsprioritäten in Einklang zu bringen (41,72%). Auch die Security-Entscheider priorisieren die Budget-Engpässe, jedoch gefolgt von der Fragmentierung oder der mangelnden Integration des Produktportfolios von Sicherheitsprodukten (43,2%) und dem Fachkräftemangel (39,81%). Während die IT-Entscheider die Fragmentierung oder mangelnde Integration des Produktportfolios im Sicherheitsbereich an die erste Stelle gesetzt haben, gefolgt von dem Fachkräftemangel (40,17%) und den Budget-Zwängen (39,74%).

  Diese Ergebnisse zeigen, wie schwierig es für die meisten Unternehmen ist, die richtige Balance zwischen den Informationssicherheitsthemen und der betrieblichen Effizienz zu finden.

- **Die Integration der Informations- und IT-Sicherheit in den Planungsprozess einer jeden neuen Entwicklung im Unternehmen ist eine wesentliche Erkenntnis der Umfrage.**

  Obwohl die meisten Unternehmen und Organisationen sich über die Vorteile von "Security by Design" einig sind, haben es nur wenige bereits in die Praxis umgesetzt. Bei dem Launch neuer Projekte und Initiativen ist die Informationssicherheit bei mehr als einem Drittel der befragten Unternehmen und Organisationen ein Aspekt, der erst nachträglich betrachtet wird. „Security by Design" ist nur bei 13% der befragten Unternehmen bereits in den Regelprozess integriert. Fast die Hälfte der befragten Entscheider (49,78%) betrachten "Security by Design" immer noch ad hoc oder von Fall zu Fall.

  Die Umfrage zeigt auch, dass 92,2% der Unternehmen Risikomanagement und Risikomodellierung in ihre Strategieplanung einbeziehen und 81,4% der Unternehmen bestätigen, dass Cyber-Security in ihrer Unternehmensmanagementstrategie widergespiegelt ist. Nur 26% der befragten Unternehmen betrachten jedoch Cyber-Security bereits bei der Planung neuer Geschäftsinitiativen.

- **Aufforderung zur Überprüfung der Governance für die Cyber-Security.**

  Der Chief Information Security Officer (CISO) sollte, um eine bessere Transparenz hinsichtlich der Geschäftsrisiken zu schaffen, eine Schlüsselrolle im Unternehmen einnehmen. Als Manager im Unternehmen ist der CISO der einzige der Cyber-Bedrohungen und Geschäftsrisiken, die von den eingesetzten Informationssystemen ausgehen, darstellen und notwendige und geeignete Lösungen aufzeigen kann. Es liegt in der Verantwortung des CISO einen risikobasierten Ansatz für die Cyber-Security im Unternehmen durch den Einsatz geeigneter Werkzeuge über alle Funktionen hinweg und vor allem durch Schärfung des Bewusstseins für die Geschäftsrisiken einzuführen. Ziel ist es, Interessenkonflikte hinsichtlich der Governance, der Leitlinien und des Managements der Cyber-Security innerhalb der Organisation zu minimieren.

Methodik: Die Unternehmensbefragung wurde vom 22. August - 19. September 2019 in Frankreich, Norwegen, Dänemark, Österreich, Deutschland, Schweiz, Belgien, Luxemburg und Saudi-Arabien durchgeführt. Im Auftrag von Devoteam befragte das IDC-Institut (IDG Group) 601 Entscheider aus europäischen und nahöstlichen Unternehmen mit mehr als 500 Mitarbeitern. Die Befragten wurden in drei unterschiedliche Kategorien unterteilt: Business (CEO, CFO, Business Manager), IT (CIO und andere IT-Manager) und Security (CISO und andere Security Manager). Die Befragten wurden zu einer Vielzahl von Aspekten angesprochen, die insbesondere mit der Herangehensweise an die Cyber-Security und der Ausrichtung ihrer diesbezüglichen Ziele insbesondere bezogen auf die digitale und geschäftliche Transformation im Unternehmen zusammenhängen.

Präambel

Da die Umfrage vor der Coronavirus-Krise durchgeführt wurde, sind die Ergebnisse umso wertvoller. Die Zunahme von Cyber-Angriffen während der COVID-19 Pandemie hat leider gezeigt, dass die Widerstandsfähigkeit im Business zunehmend auf digitale Systeme angewiesen ist und damit auf die Fähigkeiten unser Geschäft vor Bedrohungen von außen und innen zu schützen. Diese Notwendigkeit wurde durch die Krise lediglich verschärft. Die Herausforderungen für ein Unternehmen bestehen jedoch nicht darin den Schaden zu begrenzen, sondern unabhängig davon was passiert, das Geschäft aufrecht zu erhalten und wettbewerbsfähig zu bleiben.

Die Digitale Transformation kristallisiert sich auf Unternehmens-kultur und -ziele.

Alle Befragten (100%) haben bestätigt, dass bereits ein digitales Transformationsprogramm in ihrem Unternehmen ausgerollt ist. Diese Aussagen, müssen jedoch relativiert werden, da es für die Befragten nicht immer die gleiche Bedeutung hat. Für die Business Manager bedeutet Digitale Transformation in erster Linie die Schaffung neuer Produkte/ Dienstleistungen, Beschleunigung der Markteinführung (62,3%), während der gleiche Prozentsatz der IT-Entscheider meint, es gehe in erster Linie darum, die User-Experience zu verbessern um die "Loyalität und die Kundenbindung zu fördern". Gleichzeitig geht es bei fast zwei Dritteln der Security-Manager (65,9%) vor allem um den verstärkten Einsatz datengestützter Entscheidungsfindung.

Unterschiedliche Erwartungshaltung:

Business-Manager erwarten ein besseres Engagement als Priorität der Digitalen Transformation. Während die IT-Entscheider die Systemintegration als das oberste Ziel postulieren. Es überrascht nicht, dass die Security-Funktionen vor allem die Sicherheit der Informationen innerhalb der Organisation gewährleisten möchten.

Interessenskonflikte sind schwer zu überwinden. Die immanenten Merkmale der Unternehmen und die Art der mit jeder Funktion verbundenen Ziele machen es schwierig, die Gleichung "Risiken versus Agilität" zu lösen. Dies wird von allen Funktionsträgern so gesehen. Während für 62,8% der Befragten die Schaffung neuer Produkte/Dienstleistungen bzw. die Beschleunigung bei der Markteinführung als oberstes Ziel bei der Digitalen Transformation angegeben werden, sind 67% der Befragten der Ansicht, dass die Vereinbarkeit konkurrierender Prioritäten das primäre Hemmnis bei der Umsetzung einer effektiven Digitalen Transformation ist.

Cyber-Security: Das damit verbundene Risiko wird nicht so stark wahrgenommen, wie manche glauben!

Die Verbesserung der betrieblichen Effizienz wird als Primärziel von 24,96% aller Befragten genannt, dennoch wird diese nicht als Treiber der Wertschöpfung gesehen. Weitere Ziele sind die Beseitigung von Budget-Engpässen sowie die Fragmentierung und die mangelnde Integration des Sicherheitsportfolios und der Fachkräftemangel. All dies sind Gründe, die uns daran hindern Maßnahmen umzusetzen, die von den Vorschriften und Aufsichtsbehörden in diesem Bereich gefordert werden.

Die Notwendigkeit bei Unternehmen vom absoluten Begriff der Security zum relativen Begriff des Risiko Managements überzugehen.

Die Transformation sorgt dafür, dass IT Sicherheit nicht mehr als obskures und kostspieliges Hemmnis wahrgenommen wird, sondern ein objektives Kriterium für das Risiko-Management im Unternehmen darstellt. Die Umsetzung eines risikobasierten Ansatzes macht die potenziellen Auswirkungen auf das Geschäft des Unternehmens deutlich. Die Bedeutung wird für alle verständlich, messbar und vergleichbar, so dass sich Unternehmen klare Ziele und Regeln setzen müssen, um die Fortschritte bei den getätigten Investitionen auch messen zu können.

Sicherheitsthemen in die Planung von Neuentwicklungen integrieren.

Cyber-Security sollte keine Option darstellen. Insbesondere da mehr als die Hälfte der befragten Entscheidungsträger davon überzeugt sind, dass die Integration von Sicherheit in die Planung bei Neuentwicklungen eine echte Wertschöpfung darstellt. Dennoch scheint dies in der praktischen Umsetzung eine echte Herausforderung zu sein, da nur 1 von 10 Unternehmen (13%) sich mit dem Thema bereits heute auseinandersetzen, während sich weitere 50% nur von Fall zu Fall mit Cyber-Security beschäftigen.

Die Nutzung eines risikobasierten Ansatzes um geschäftliche Auswirkungen deutlich zu machen, ist der wesentliche Ausgangspunkt für ein wirksames Risiko-Management im Allgemeinen und ein wirksames Management der Cyber-Security im Besonderen.

Eine Metamorphose ist im Gange - aber die Verlockung eines hohen Gewinns bleibt.

Wenn es um Sicherheit von Informationssystemen und von Netzen geht, beginnen sich die Linien zu verschieben. Sicherheit sollte nicht das Geschäft eines einzelnen Mitarbeiters sein, sondern ein integraler Bestandteil der Kultur einer jeden Abteilung. Unternehmen und Organisationen haben bereits in einer Startphase begonnen zu digitalen Plattformen zu migrieren. Über alle Funktionen betrachtet integrieren fast 26% der Unternehmen die Sicherheit von Systemen und Netzen bereits in der Entwicklungsphase (37,7% der Business-Funktionen, 27,3% der Security-Funktionen und 23,2% der IT-Funktionen).

Unabhängig vom Versprechen einer sicheren Transformation der Arbeitsplätze, neigen Organisationen in einem zunehmend wettbewerbsorientierten Marktumfeld immer noch dazu, die Anwendersicherheit gegenüber der Unterstützung von Geschäftsinitiativen zu vernachlässigen. Der CIO ist besser auf regulatorische Risiken vorbereitet als auf die Risiken der Anwendersicherheit.

Cyber-Security-Governance überdenken, um den Wandel zu beschleunigen

Während CIOs und CISOs auf einer gemeinsamen Linie liegen was den Nutzen und die formale Herangehensweise an die Sicherheitsthemen angeht, unterscheiden sich ihre Ansichten jedoch wesentlich wenn sie gefragt werden, was im Hinblick auf die betriebliche Sicherheit notwendig und wichtig ist.

Security Manager legen großen Wert auf die unternehmensweite Integration von Sicherheit (Integration und Optimierung zur Unterstützung des Geschäfts). IT-Manager verstehen die Herausforderung, ein engagiertes Team zu unterhalten, und sie sind eher bereit, wichtige Sicherheitsbereiche an Dienstleister auszulagern.

Der CISO - der unentbehrliche Vermittler

Mit einer besseren Vision über potentielle Risiken ist der CISO ein wichtiger Akteur im Unternehmen, da nur der CISO in der Lage ist, Cyber-Bedrohungen in Geschäftsrisiken zu transformieren und auch geeignete Lösungen zur Prävention zu empfehlen. Es liegt in der Verantwortung des CISO einen risikobasierten Ansatz der Cyber-Security in die Unternehmen zu tragen und durch geeignete Werkzeuge und vor allem durch Schärfung einer Risiko- / Security-Kultur über alle Ebenen der Organisation hinweg zu verbreiten.

In der Tat ist dies die Hauptrolle, die dem CISO von den befragten Entscheidungsträgern zugewiesen wird: Kooperieren mit Geschäftsbereichen zur Förderung von Aktivitäten innerhalb einer vereinbarten Risikobereitschaft (47%), vor der Verringerung der Wahrscheinlichkeit von (internen und externen) Bedrohungen, die das Unternehmen und seine Vermögenswerte gefährden (45%) und der Integration der Sicherheit in das Unternehmensumfeld, um Kosten- und Effizienzvorteile zu steigern (43%).

„[…] es ist von grundlegender Bedeutung, die Leitlinien der Cyber-Security neu zu überdenken. Die Trennung der IT- und Security-Rollen vermeidet beispielsweise vorhandene Interessenkonflikte. Der CISO sollte dann in der Lage sein, das notwendige Buy-In sowohl von Business Managern als auch von der Geschäftsleitung zu erhalten. Auf der Grundlage dieser Vereinbarung kann der CISO Anforderungen an die IT festlegen, die dann als Dienstleister mit einem formellen Auftrag diese erfüllen", erklärt Martin Esslinger, Partner bei Devoteam

Weitere Informationen:

Die vollständige Umfrage wird in Form von 3 Whitepapers zur Verfügung gestellt. Die Aufteilung auf drei Whitepapers geschieht nicht um einen Spannungsbogen zu schaffen, sondern um die jeweils grundlegenden Tendenzen der Umfrage besser hervorheben zu können. Das erste Whitepaper betrifft das Risikomanagement und die geschäftlichen Auswirkungen, das zweite die Sicherung der Digitalen Transformation und die Digitalisierung der Security, und die dritte DevSecOps und die operative Exzellenz der Sicherheit.

Über Devoteam

Devoteam bietet innovative Technologieberatung für Unternehmen.

Als professioneller Partner (Pure Player) für die digitale Transformation führender Organisationen in der gesamten EMEA-Region setzen sich unsere mehr als 7.600 Fachleute dafür ein, dass unsere Kunden ihre "Digital Battles" gewinnen. Mit unserer einzigartigen Transformations-DNA verbinden wir das Geschäft und die Technologie.

Mit unserer Präsenz in 18 Ländern in Europa und im Nahen Osten und unserer mehr als 20-jährigen Erfahrung entwickeln wir bedarfsorientierte technologische Lösungen und schaffen so einen Mehrwert für unsere Kunden, Partner und Mitarbeiter

Devoteam erzielte im Jahr 2019 einen Umsatz in Höhe von 761,9 Millionen €.

Wir bei Devoteam sind Digital Transformakers.

Devoteam SA (DVT) ist im B-Fach der Euronext Paris (ISIN: FR 0000073793) gelistet, als Teil der Indizes CAC All Shares, CAC All-Tradables, CAC Mid&Small, CAC Small, CAC SOFT. & C.S., CAC TECHNOLOGY und ENT PEA-PME 150.

Über IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,000 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 90 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly-owned subsidiary of International Data Group (IDG), the world's leading tech media, data and marketing services company.

Ansprechpartner für die Redaktionen
Devoteam GmbH
Jürgen Martin
Gutenbergstraße 10
D-64331 Weiterstadt

Phone: +49 6151 868-7487
Fax: +49 6151 868-7131
E-Mail: info@devoteam.de
Internet: https://de.devoteam.com