

09.11.2020 - 07:05 Uhr

Cybersecurity aufgrund von COVID-19 mehr denn je im Fokus von Führungskräften

Die Schweizer Ergebnisse einer weltweiten PwC-Befragung zum Thema Cybersecurity (PwC's Global Digital Trust Insights Survey: "Cybersecurity comes of age")

Cybersecurity aufgrund von COVID-19 mehr denn je im Fokus von Führungskräften

- **Weltweite PwC-Untersuchung: 96% von über 3000 befragten Unternehmen haben ihre Cybersecurity-Strategie aufgrund von COVID-19 geändert - in der Schweiz sind es 89%.**
- **Steigende Budgets trotz Umsatzrückgang: 34% der befragten Unternehmen in der Schweiz wollen ihre Cyberbudgets für 2021 erhöhen.**
- **50% der befragten Schweizer Unternehmen sehen einer Beschleunigung der Digitalisierung aufgrund von COVID-19 entgegen.**
- **Cyber-Risikofaktoren 2021: Fast 80% der befragten Unternehmen in der Schweiz befürchten Ransomware-Angriffe und Cyberattacken auf Cloud Services mit erheblichen Folgen.**

Zürich, 9. November 2020 - Cybersicherheit ist zweifelsohne in der Chefetage angekommen. Innerhalb von wenigen Jahrzehnten hat das Thema - auch getrieben durch die steigende Zahl der erfolgreichen Cyberattacken der letzten Monate - immens an Bedeutung gewonnen und sich damit zum strategischen Partner in den Unternehmen entwickelt. Das zeigen die Ergebnisse der Umfrage "PwC Digital Trust Insights 2021", bei der weltweit über 3000 Führungskräfte aus Wirtschaft und Technologie zur Entwicklung von Cybersicherheit befragt wurden - auch unter Berücksichtigung der Corona-Pandemie. 50% der befragten Unternehmen weltweit geben an, Cybersicherheit und Datenschutz in jeder Geschäftsentscheidung zu berücksichtigen, was eine Verdopplung zum Vorjahreswert (25%) ausmacht.

Resilienz für jedes Szenario

Die Verankerung von Cybersicherheit in den Geschäftsprozessen ist dringender als je zuvor, denn die COVID-19-Pandemie hat die Digitalisierung weltweit beschleunigt und damit auch die Angriffsfläche für Cyberattacken erweitert. Dies bestätigen auch 50% der weltweit befragten Unternehmen. Die grössten Risikobereiche sehen die Befragten bei der Nutzung von Cloud und Mobile-Diensten sowie bei Social Engineering. Zum Teil halten weit mehr als die Hälfte der Befragten Angriffe hier für sehr wahrscheinlich; fast 80% erwarten sogar erhebliche negative Auswirkungen auf das eigene Unternehmen durch Cyberattacken mittels Ransomware- und Disruptionware. "Die grösste Gefahr geht hierbei eindeutig von Cyberkriminellen aus", so Johannes Dohren, Director Incident Response Cybersecurity bei PwC Schweiz. Um auf alle Risikoszenarien vorbereitet zu sein, wollen 30% der Führungskräfte mehr in fortgeschrittene Technologien und Automation investieren, um die Wirksamkeit der Cyberabwehr zu erhöhen. Ausserdem ist bei 71% der befragten Unternehmen geplant, vermehrt Stresstests durchzuführen, um sicherzustellen, dass ihre kritischen Unternehmensfunktionen im Falle eines aggressiven Cybervorfalles weiterhin funktionieren, respektive rasch wiederhergestellt werden können, um den Business Impact möglichst gering zu halten. "Die Orchestrierung einzelner Funktionen für Geschäftskontinuität, Wiederherstellung nach einem Notfall und Krisenmanagement wird für die meisten Organisationen zum Schlüsselfaktor für eine höhere Resilienz. Cyberresilienz ist kein IT- oder IT-Security-Thema allein.", so Urs Küderli, Partner und Leiter Cybersecurity and Privacy, PwC Schweiz.

Cyberstrategie mit neuen Ansätzen

Die veränderte Risikolage durch die COVID-19-Pandemie hat die Cyberstrategien nahezu aller weltweit befragten Unternehmen beeinflusst (96%). Über 50% der Befragten geben an, dass sie begonnen haben, neue Ansätze zur Cybersicherheit zu implementieren und sogar jede fünfte Organisation erkennt bereits erste Vorteile. Die in der Schweiz befragten Führungskräfte sehen besonders den Einsatz von Virtualisierung (27%) und von Künstlicher Intelligenz zur Cyberabwehr (14%) als vielversprechend und wirksam an. Zukünftig wollen sich die Befragten ausserdem über die Geschäftskontinuitätsplanung hinaus auch stärker mit Cyberabwehr beschäftigen (32%), ein modernes Identitäts- und Zugriffsmanagements (29%) sowie ein integriertes System Cloud- und Netzwerksicherheit implementieren.

Mit mehr Budget und Kompetenzen zu digitalem Vertrauen

Angetrieben durch die COVID-19-Pandemie verändert die Digitalisierung weite Teile des Unternehmens. Für 38% der befragten Unternehmen in der Schweiz ist die Effizienzsteigerung bestehender Prozesse das Hauptziel, gefolgt von der Modernisierung der Organisation mit neuen Fähigkeiten (32%). Spezifisch im Cyberbereich soll in Zukunft die verbesserte Messbarkeit bei der Quantifizierung von Cyberrisiken (36%) optimiert werden, um die Wahrscheinlichkeit von zunehmend komplexeren Cyberangriffen besser einschätzen und der Geschäftsleitung besser visualisieren zu können. Hier zu meint Fabian Faistauer, Experte für Cyber Compliance Monitoring bei PwC Schweiz: "Ein transparentes unternehmensinternes Reporting von bestehender Cyberrisiken und Schwachstellen ist essenziell für das Wahrnehmen der Verantwortlichkeit und somit der erste Schritt der Risikominimierung."

Die Vorstandsetage hat erkannt, dass neue Geschäftsfelder und die digitale Transformation nachhaltig zu sichern, nicht möglich

ist, ohne ein hohes Mass an Cybersicherheit: 25% der befragten CEOs in der Schweiz geben an, dass sie häufiger mit dem Chief Information Security Officer (CISO) in Kontakt treten. Da der CISO daneben am häufigsten dem Chief Information Officer, dem Verwaltungsrat und dem Chief Risk Officer rapportiert, werden ihm zunehmend erweiterte Fähigkeiten zuteil: Innovationsförderung, das Mentoring von Mitarbeitern und die Risikobeurteilung zählen in diesen Zeiten zu den Top 3 der am meisten geschätzten Fähigkeiten der CISO.

Die steigende Bedeutung von Cybersicherheit zeigt sich zudem bei der Budget- und Ressourcenplanung. Mehr als die Hälfte der weltweit befragten Unternehmen wollen ihre Cyberbudgets erhöhen und ihre Mitarbeiterzahl im Bereich Cybersicherheit aufstocken - und das obwohl die prognostizierten Umsätze der Unternehmen aufgrund von COVID-19 auch für 2021 noch deutlich sinken (59%Schweiz/ 64% Global).

"Die Neuausrichtung der Cyberstrategie definiert nicht nur die wachsende Rolle der CISO, sondern wirkt sich auch auf die Art und Weise aus, wie die Organisation Cyberbudgets festlegt, in Sicherheitslösungen investiert, Pläne für die Ausfallsicherheit erstellt und ihre Sicherheitsorganisation verbessert. Sie bestimmt, ob die Geschäftsführung digitales Vertrauen schaffen kann, das ihre Organisationen mit Strategien zum Schutz und zur Wertschöpfung sicher in die Zukunft führt", kommentiert Urs Küderli.

Über die Studie

[Klicken Sie hier](#), um zu den PwC Global Digital Trust Insights mit detaillierten Informationen und Resultanten zu gelangen. Für die Studie wurden im Juli und August 2020 weltweit 3249 Führungskräfte aus den Bereichen Wirtschaft, Technologie und Sicherheit (CEOs, Corporate Directors, CFOs, CISOs, CIOs und C-Suite-Verantwortliche) zur Entwicklung und Zukunft von Cybersicherheit befragt. 34% der befragten Unternehmen sind in Westeuropa ansässig, davon 5.2% in der Schweiz, gefolgt von Nordamerika (29%), Asien-Pazifik (18%), Lateinamerika (8%), Osteuropa (4%), Naher Osten (3%) und Afrika (3%). Um die globalen Ergebnisse der Studie einsehen zu können (englischsprachig), klicken Sie bitte [hier](#).

Über PwC

Der Zweck von PwC ist es, das Vertrauen in der Gesellschaft aufzubauen und wichtige Probleme zu lösen. Wir sind ein Netzwerk von Firmen, das in 157 Ländern über 284'000 Mitarbeitende beschäftigt. Diese setzen sich dafür ein, in den Bereichen Wirtschaftsprüfung, Beratung und Steuern erstklassige Dienstleistungen zu erbringen. PwC Schweiz hat über 3250 Mitarbeitende und Partner an 14 verschiedenen Standorten in der Schweiz und einem im Fürstentum Liechtenstein. Erfahren Sie mehr und sagen Sie uns, was für Sie wichtig ist, unter www.pwc.ch. "PwC" bezieht sich auf das PwC-Netzwerk und/oder eine oder mehrere seiner Mitgliedsfirmen, von denen jede ein eigenständiges Rechtssubjekt ist. Nähere Angaben dazu finden Sie unter www.pwc.com/structure.

Diese Meldung kann unter <https://www.presseportal.ch/de/pm/100008191/100859141> abgerufen werden.