PRESSEINFORMATION

Lösegeld statt Compliance: Schweizer Unternehmen vertuschen Nichteinhaltung von Gesetzen eher

Au ZH, Schweiz, 26. Juni 2019 – D**ie Einhaltung der gesetzlichen und vertraglichen Regelungen im Bereich der IT** ist für den Datenschutz und die IT-Sicherheit unerlässlich. Dennoch gehen Schweizer Unternehmen eher auf Lösegeldforderungen ein statt Strafen für die Nichteinhaltung zu zahlen. So das erschreckende Ergebnis des aktuellen Risk:Value-Report von NTT **Security (Switzerland).**

Den jährlichen Risk:Value-Report erstellt das Marktforschungsunternehmen Jigsaw Research im Auftrag von NTT Security, dem auf Sicherheit spezialisierten Unternehmen und „Security Center of Excellence" der NTT Group (NYSE: NTT). Dafür geben weltweit Führungskräfte – in diesem Jahr 2.256 – ihre Einschätzungen zu Themen rund um IT und IT-Sicherheit ab.

Bei der aktuellen Untersuchung zeigt sich, dass im Vergleich zum Vorjahr mehr Schweizer Unternehmen im Falle eines Sicherheitsvorfalls Lösegeld an die Hacker zahlen würden, als stärker in die Informationssicherheit zu investieren, da sie ein solches Vorgehen für kostengünstiger halten: Im vergangenen Jahr gaben 23% der befragten Entscheidungsträger an, bei einer Ransomware-Attacke lieber auf die Forderungen der Angreifer einzugehen, in diesem Jahr sind es sogar 40%. Das korreliert mit der Aussage, dass 44% der Schweizer Unternehmen eher Lösegeld als eine Strafe dafür zahlen würden, dass sie nicht die geltenden Gesetze und Richtlinien eingehalten haben. „Dieses Ergebnis ist mehr als erschreckend, gerade auch angesichts der nicht abebbenden Gefahr von Ransomware-Angriffen", erklärt Kai Grunwitz, Senior Vice President EMEA bei NTT Security. „Wenn sich Unternehmen nun von der Bezahlung von Lösegeld Kostenvorteile versprechen, ist das in unseren Augen mehr als trügerisch. Und das böse Erwachen wird früher oder später für viele kommen."

Dabei sind sich die Unternehmen der drohenden Gefahr durchaus bewusst: Laut den befragten Entscheidungsträgern stellen Cloud (24%), BYOD (20%), Ransomware (18%) und IoT (12%) in den nächsten 12 Monaten eine mögliche Bedrohung dar. Fast zwei Drittel fürchtet jedoch, dass die Sicherheitslücke innerhalb des Unternehmens liegt: Böswillige Insider-Bedrohungen wie Datendiebstahl (30%), versehentliche oder fahrlässige Sicherheitslücken (28%), aber auch eine Schatten-IT (16%) und Phishing (36%) stufen die Befragten als potentielles Sicherheitsrisiko ein.

Wenig überraschend ist, dass lediglich 42% der Unternehmen bereits über einen Incident-Response-Plan verfügen; immerhin 38% stecken laut Studie im Implementierungsprozess und weitere 10% planen die Umsetzung entsprechender Maßnahmen in naher Zukunft (Abbildung 1). „In den vergangenen Jahren hat sich in den Unternehmen bezüglich des Incidet-Response-Plans trotz zahlreicher bekannt gewordener Sicherheitsvorfälle und ständig zunehmendem Schadenspotential nicht viel geändert. Obwohl nur mit dedizierten Ablauf- und Notfallplänen angemessen und schnell auf IT-Sicherheitsvorfälle reagiert werden kann, verfügt noch immer nicht mal die Hälfte der befragten Unternehmen über einen Incident-Response-Plan", fasst Grunwitz zusammen. „Auch die erfreulich hohe Zahl laufender Implementationen und Projekten in Planung ist bei genauer

Betrachtung ernüchternd: die vergangenen Studien machen deutlich, dass sie oft nur Compliance getrieben sind und reine Absichtserklärungen bleiben, die nicht zu einer signifikanten Verbesserung der Incident-Response-Readiness der Unternehmen im Folgejahr führen – nur wenige dieser Incident-Response-Projekte werden erfolgreich umgesetzt (Abbildung 2). Die Zusammenarbeit mit einem erfahrenen Incident-Response-Partner ist darum dringend zu empfehlen."

Auch bezüglich der Sicherheitsrichtlinien sieht es nicht besser aus. Erst rund die Hälfte der Unternehmen (48%) haben vollständige Sicherheitsrichtlinien eingeführt. 21% haben ihre Mitarbeiter allerdings nicht aktiv über die Richtlinien informiert. „Es ist unerlässlich, die Mitarbeiter ausreichend über die Gefahren und den richtigen Umgang mit ihnen zu schulen – vor allem da Social-Engineering-Angriffe immer beliebter werden. Jeder Mitarbeiter wird schnell zur Sicherheitslücke, wenn er keine sehr gute Security-Awareness besitzt. Unternehmensspezifische Awareness-Trainings können für die Thematik sensibilisieren und ihnen Sicherheit im Umgang mit entsprechenden Vorfällen bieten", betont Grunwitz.

Der Austausch innerhalb des Unternehmens zum Thema Sicherheit muss überhaupt deutlich steigen: Nur 66% der befragten Entscheidungsträger gaben an, auf dem aktuellen Stand bezüglich Attacken, potentiellen Attacken und der Compliance in ihrem Unternehmen zu sein. Das korreliert mit der Aussage, dass nur in 68% der Unternehmen Sicherheit ein regulärer Punkt bei der Vorstandssitzung ist. Dass zudem 46% schon von einem Sicherheitsvorfall betroffen waren, dennoch 42% der Befragten davon ausgehen, nie in diese Situation zu kommen, unterstreicht, dass sie sich der Gefahr noch bewusster werden müssen. Über die gravierenden negativen Auswirkungen, die ein Sicherheitsvorfall mit Datendiebstahl hat, sind sich die befragten Unternehmen schliesslich durchaus bewusst: Genannt wurden Verlust des Kundenvertrauens (42%) Beeinträchtigung der Reputation (38%) und finanzielle Einbussen (36%).

Das „Risk:Value Executive Summary" steht zum Download unter https://www.nttsecurity.com/de-de/risk-value-report-2019 zur Verfügung.

Methodologie

Die Risk:Value-Studie wurde im Auftrag von NTT Security zwischen Februar und März 2019 vom Marktforschungsunternehmen Jigsaw Research durchgeführt. Dabei wurden 2.256 Nicht-IT-Entscheider in Deutschland, Österreich, Großbritannien, Benelux, Frankreich, Italien, Norwegen, Spanien, Schweden, der Schweiz sowie in Chile, Brasilien, Australien, Hongkong, Indien, Japan, Singapur und den USA befragt. Die befragten Unternehmen sind unter anderem in den Bereichen Manufacturing, Handel, Healthcare, Logistik, Telekommunikation und Verwaltung tätig und beschäftigen mehr als 250 Mitarbeiter.

Abbildungen:

Abbildung 1: (IR-Plan_CH_2019.JPG)

Bildunterschrift: Verfügbarkeit von Incident-Response-Plänen in Schweizer Unternehmen 2019

Abbildung 2: (IR-Readiness_DACH_2017-19.JPG)

Bildunterschrift: Entwicklung der Incident Response Readiness der DACH-Unternehmen von 2017–2019

Über Jigsaw Research

Jigsaw Research ist ein internationales Marktforschungsinstitut, das sich zur Aufgabe gemacht hat, das menschliche Verhalten zu analysieren. Das erfahrene Team greift dafür auf Forschungstechniken zurück, die sowohl bewusstes als auch unbewusstes Verhalten beleuchten.

Über NTT Security

NTT Security ist das auf Sicherheit spezialisierte Unternehmen und „Security Center of Excellence" der NTT Group. Mit „Embedded Security" bietet NTT Security Kunden zuverlässige Lösungen für ihre Anforderungen in der digitalen Transformation. NTT Security verfügt über 10 SOCs, sieben Zentren für Forschung und Entwicklung sowie mehr als 1.500 Sicherheitsexperten und behandelt jährlich Hunderttausende Sicherheitsvorfälle auf sechs Kontinenten.

NTT Security sichert eine effiziente Ressourcennutzung, indem Kunden der richtige Mix an ganzheitlichen Managed Security Services, Security Consulting Services und Security-Technologie zur Verfügung gestellt wird – unter optimaler Kombination von lokalen und globalen Ressourcen. NTT Security ist Teil der NTT Group (Nippon Telegraph and Telephone Corporation), einem der grössten IKT-Unternehmen weltweit. Weitere Informationen über NTT Security finden sich unter http://www.nttsecurity.com/ch. Informationen zur globalen NTT Group finden sich unter www.ntt-global.com.

Bei Rückfragen wenden Sie sich bitte an:

NTT Security

Romy Däweritz
Marketing Manager DACH
Tel.: +49 89 945730
romy.daeweritz@nttsecurity.com hakan.cakar@nttsecurity.com

PR-COM GmbH

Christina Haslbeck
Account Manager
Tel.: +49 89 59997 702
christina.haslbeck@pr-com.de