Kontinuierliche Herausforderung IT-Sicherheit

Neues IT-Sicherheitsgesetz zwingt den GFGH jetzt zum schnellen Handeln

→ IT-Sicherheit ist kein Thema, das man einmalig abarbeitet und dann als erledigt betrachtet. Vielmehr erfordert es ständige Aufmerksamkeit und kontinuierliche Bemühungen. Das neue IT-Sicherheitsgesetz, das im Oktober in Kraft treten wird, erfordert jetzt rasches Handeln, weil es Getränkefachgroßhändler – sie gehören zur kritischen Infrastruktur und/oder beliefern kritische Infrastruktur – dazu verpflichtet, nachhaltige Sicherheitsmaßnahmen zu implementieren, zu dokumentieren und jederzeit nachzuweisen zu können.

Die Bedrohungen, denen der Getränkefachgroßhandel ausgesetzt ist, sind vielfältig. Eine Verschlüsselung durch Ransomware kann ein Unternehmen praktisch lahmlegen, da Bestellungen oft per E-Mail oder EDI ins System gelangen. Ohne eine funktionierende IT-Infrastruktur wird ein Betrieb schnell handlungsunfähig. Auch der Verlust und die Veröffentlichung sensibler Daten können gravierende Konsequenzen haben, von Vertrauensverlust bis hin zu rechtlichen Problemen.

Das neue IT-Sicherheitsgesetz zielt darauf ab, diese Bedrohungen zu minimieren, indem es Unternehmen zur Ergreifung angemessener Sicherheitsmaßnahmen verpflichtet. Unternehmen müssen nachweisen, dass sie ausreichende Vorkehrungen zum Schutz vor Cyber-Kriminalität getroffen haben. Andernfalls drohen empfindliche Strafen, wobei die Verantwortung direkt bei der Geschäftsführung liegt. Dies erhöht den Druck auf Unternehmen, ihre IT-Sicherheit erheblich zu verbessern und kontinuierlich zu überprüfen.

Kontinuierliche Sicherheitsmaßnahmen statt Einmalaufwand

Matthias Helm vom auf IT-Sicherheit spezialisierten Dienstleister Team Business IT betont: „IT-Sicherheit ist kein Projekt, das man in einer Woche abschließt. Die Bedrohungslage ändert sich ständig, und Sicherheitsmaßnahmen müssen kontinuierlich überprüft und angepasst werden. Eine einmalige Aktion reicht nicht aus."

Sicherheitsexperte Christian Voigt ergänzt: „Es ist viel effektiver, sich regelmäßig, beispielsweise monatlich oder vierteljährlich, mit IT-Sicherheit zu beschäftigen. Diese kontinuierliche Herangehensweise sorgt dafür, dass Sicherheitslücken laufend erkannt und geschlossen werden können, bevor sie zu ernsthaften Problemen führen."

Die Notwendigkeit externer Unterstützung

Die Komplexität der IT-Sicherheit erfordert immer externen Rat. Helm zieht einen Vergleich zu den regelmäßigen Schulungen für Lkw-Fahrer: „Wie Lkw-Module, die Fahrer

Rechtzeitig Vorischtsmaßnahmen treffen!

Dirk Reinsberg, Geschäftsführender Vorstand des BV GFGH

„Wie wichtig die Absicherung der unternehmenseigenen IT ist, führen uns fast tägliche Schlagzeilen über Cyberangriffe vor Augen. Gehackte Unternehmes-IT, Passwörter ausspioniert, Betrug beim Online-Handel: Mehr als jedes dritte Unternehmen wird in Deutschland von Hackern angegriffen. Dieser Bedrohungslage gilt es als Unternehmer aktuell mehr als denn je entgegenzutreten."

jährlich absolvieren müssen, sollte auch die IT-Sicherheit regelmäßig aufgefrischt werden. Externe Experten können dabei helfen, das notwendige Wissen und die aktuellen Bedrohungen im Blick zu behalten. Die Zusammenarbeit mit spezialisierten Dienstleistern wie Team Business IT bietet entscheidende Vorteile. Wir bringen sowohl IT-Kompetenz als auch Branchenkenntnis mit und gehen gezielt auf die Bedürfnisse des Getränkefachgroßhandels ein."

Die aktuelle Lage der IT-Sicherheit im Getränkefachgroßhandel

Im Getränkefachgroßhandel ist die Versorgungslage in Sachen IT-Sicherheit sehr unterschiedlich. Viele Unternehmen sind sich der Bedeutung von IT-Sicherheit bewusst, doch die Umsetzung variiert stark. Während einige meinen, mit einer Firewall und Virenschutz ausreichend abgesichert zu sein, sind diese Maßnahmen allein nicht mehr genug.

Der Arbeitsalltag im Getränkefachgroßhandel lässt wenig Raum für umfangreiche Sicherheitsüberlegungen. Greifbare Probleme wie defekte Infrastruktur oder dringende betriebliche Anliegen nehmen oft Vorrang. Diese Themen erscheinen unmittelbarer und dringlicher als die abstrakte Bedrohung durch Cyberkriminalität. Dies führt dazu, dass viele Unternehmen erst reagieren, wenn bereits ein Schaden eingetreten ist, was dann oft zu spät ist – das neue Gesetz wirkt diesem Verhalten entgegen.

Ein weit verbreitetes Missverständnis ist, dass mittelständische Unternehmen weniger attraktiv für Cyber-Angriffe seien. Diese Annahme kann gefährlich sein, da jede Sicherheitslücke in alltäglicher Software ein Einfallstor für Angreifer darstellt.

Die zunehmende Raffinesse der Angreifer

Cyber-Kriminelle werden immer raffinierter und nutzen oft unbewusste Schwachstellen in der IT-Infrastruktur aus. Phishing-Angriffe, bei denen Mitarbeitende durch gefälschte E-Mails dazu gebracht werden, Zugangsdaten preiszugeben, sind alltäglich. Cyber-Kriminalität wird dabei immer mehr zu einem lukrativen Geschäft, bei dem mit minimalem Aufwand maximaler Schaden verursacht wird.

Ransomware-Attacken können den Betrieb von einem Moment auf den anderen lahmlegen und enorme Kosten verursachen, sei es durch direkte Zahlungen an Erpresser oder durch den Ausfall des Geschäfts. Selbst etablierte Gegenmaßnahmen wie eine gute Backup-Strategie reichen häufig nicht aus, um die Schäden zu begrenzen.

Einfache Maßnahmen mit großer Wirkung

Ein speziell zur Vorbereitung auf die neuen gesetzlichen Anforderungen angepasster Sicherheits-Check von Team Business IT bewertet 15 Themen mit einem Ampelsystem und zeigt klar, wo Handlungsbedarf besteht. Diese Einschätzung hilft den Unternehmen, gezielte Maßnahmen zu ergreifen und ihre Sicherheitslage zu verbessern, entweder mit Bordmitteln oder mit externer Unterstützung.

Oft sind es einfache, aber wichtige Maßnahmen, die große Wirkung haben können. Zum Beispiel, dass die Tür zum Serverraum immer verschlossen ist; oder regelmäßige Schulungen für alle, die dem Betrieb angehören. Ein monatliches Sicherheitstraining von nur 15 Minuten kann erheblich zur Sensibilisierung und Verbesserung der Sicherheitskultur beitragen.

Fazit Langfristige Sicherheit durch kontinuierliche Betreuung

IT-Sicherheit im Getränkefachgroßhandel erfordert eine langfristige und kontinuierliche Herangehensweise. Regelmäßige Schulungen und Überprüfungen sind notwendig, um die Sicherheit aufrechtzuerhalten und sich gegen die ständig wachsenden Bedrohungen zu wappnen. Externe Unterstützung, wie sie Team Business IT bietet, ist dabei unverzichtbar, um die Komplexität der IT-Sicherheit zu meistern und den gesetzlichen Anforderungen gerecht zu werden.

Hintergrund: Team Business IT mit Sitz in Bremen und Rostock beschäftigt rund 60 Mitarbeitende. Der Dienstleister betreut den Getränkefachgroßhandel in allen Sicherheitsfragen und ist auf die Getränkebranche spezialisiert. Zur Vorbereitung auf das IT-Sicherheitsgesetz, das im Herbst 2024 in Kraft tritt, bietet das Unternehmen einen Check, der Handlungsbedarf aufzeigt und bei der Umsetzung begleitet. Die Leistung steht allen Unternehmen frei, unabhängig von einer Mitgliedschaft in Team Beverage Verbundgruppen.
www.teambusinessit.de

→ MATTHIAS HELM
Er ist Geschäftsführer von Team Business IT und verfügt über langjährige Erfahrung in der IT-Branche und der Getränkefachgroßhandelsbranche. Unter seiner Leitung hat Team Business IT zahlreiche Projekte zur Verbesserung der IT-Sicherheit und Effizienz von Unternehmen in der Getränkeindustrie erfolgreich umgesetzt. (Bild: Team Business IT/Team Beverage AG)

→ CHRISTIAN VOIGT
Er ist Sicherheitsexperte bei Team Business IT. Mit einem Hintergrund in Informationssicherheit und umfangreicher Erfahrung im Bereich IT-Security, berät er Unternehmen im Getränkefachgroßhandel und hilft ihnen, ihre IT-Infrastrukturen gegen die zunehmenden Bedrohungen durch Cyberkriminalität zu schützen. (Bild: Team Business IT/Team Beverage AG)