2N STÄRKT RICHTLINIEN ZUR CYBERSICHERHEIT NACH NEUESTEN UNTERSUCHUNGEN ZUR CYBERKRIMINALITÄT

- Der Cyber Readiness Report 2021 von Hiscox zeigt, dass die Cyber-Bedrohung für Unternehmen zunimmt, wobei die Zugangskontrolle für viele Unternehmen eine Schwachstelle darstellt
- Während des Europäischen Monats der Cybersicherheit 2020 hat 2N einen Leitfaden für Unternehmen veröffentlicht, um sie bei der Verhinderung von Cyberangriffen zu unterstützen. Im Oktober 2021 wurde der Leitfaden als Reaktion auf die wachsenden Bedrohungen verstärkt.

Anlässlich des Europäischen Monats der Cybersicherheit 2021 hat 2N, weltweit führender Anbieter von IP-Zugangskontrollsystemen, seinen Leitfaden verschärft, um Verbraucher und Gebäudemanager bei der Verhinderung von Cyberangriffen zu unterstützen. Dieser Schritt ist eine Reaktion auf die Tatsache, dass die Bedrohung durch Cyberkriminalität zunimmt und die Zugangskontrolle eine häufige Schwachstelle bleibt.

Anfang des Jahres veröffentlichte Hiscox seinen „Cyber Readiness Report 2021“. Er basiert auf einer Umfrage unter mehr als 6.000 Unternehmen in den USA, dem Vereinigten Königreich, Spanien, den Niederlanden, Deutschland, Frankreich, Belgien und Irland. Der Bericht bestätigt, dass sich die Ausgaben für Cybersicherheit pro Unternehmen in den letzten zwei Jahren mehr als verdoppelt haben, was eine direkte Reaktion auf die zunehmende Bedrohung darstellt. Fast die Hälfte der Befragten gab an, dass ihr Unternehmen seit Beginn der Pandemie anfälliger für Cyberangriffe geworden sei, wobei der Anteil der Unternehmen mit mehr als 250 Mitarbeitern auf 59 Prozent stieg. 28 Prozent der befragten Unternehmen, die von Angriffen betroffen waren, wurden im vergangenen Jahr mehr als fünf Mal angegriffen. Jedes sechste Unternehmen, das Opfer von Cyberkriminalität wurde, gab an, dass ein Cybervorfall die Lebensfähigkeit seines Unternehmens bedroht.

Hiscox bewertete den Reifegrad der Unternehmen in sechs verschiedenen Bereichen, die die für die Installation, den Betrieb, die Verwaltung und die Kontrolle eines wirksamen Sicherheitssystems erforderlichen Elemente umfassen. Einer dieser sechs Bereiche war das „Identitäts- und Zugangsmanagement“, das bei allen untersuchten Unternehmen an zweiter Stelle der Liste stand.

Als Reaktion auf diese Ergebnisse hat 2N seinen Leitfaden zur Vorbeugung von Cyberangriffen für Verbraucher und Gebäudemanager erweitert. Dieser wurde erstmals während des Europäischen Monats der Cybersicherheit 2020 veröffentlicht. Zwei neue Ratschläge wurden hinzugefügt:

1. Halten Sie sich an ein bewährtes Sicherheitskontrollsystem. Zwei der angesehensten sind ISO 27001 und SOC 2. Sie dienen Unternehmen als Leitfaden für die Schaffung sicherer Systeme und Prozesse.

2. Vergewissern Sie sich, dass das Zugangskontrollsystem die Verwendung von Verschlüsselung und mehrstufiger Authentifizierung umfasst. Dies schützt die Kommunikation zwischen Geräten, Controllern und mobilen Geräten und stellt sicher, dass es keine Hintertüren für „Wartungszwecke“ gibt.

Tomáš Vystavěl, Chief Product Officer bei 2N, sagt: „Wir waren der Meinung, dass es notwendig war, unseren Leitfaden zur Cybersicherheit zu verstärken, zum einen, weil die Bedrohung zunimmt, zum anderen aber auch, weil viele Unternehmen bei der Cybersicherheit im Bereich der Zutrittskontrolle immer noch „aufholen“ müssen. Das ist wichtig, denn wenn das Zugangskontrollsystem kompromittiert wird, ist der tägliche Betrieb des Gebäudes – und damit auch der Bewohner – unmittelbar gefährdet. Die Einstellungen ändern sich, aber sie müssen sich noch schneller ändern.

Die vollständige Liste der Ratschläge von 2N zur Verhinderung von Cyberangriffen finden Sie weiter unten.

Weitere Einzelheiten über den Ansatz von 2N zur Cybersicherheit: https://www.2n.cz/en_GB/about-2n/cybersecurity

RATSCHLÄGE VON 2N ZUR VERHINDERUNG VON CYBERANGRIFFEN

1. Verfolgen Sie die Einhaltung eines bewährten Sicherheitskontrollrahmens. Zwei der angesehensten sind ISO 27001 und SOC 2. Sie dienen Unternehmen als Leitfaden für die Entwicklung sicherer Systeme und Prozesse.
2. Vergewissern Sie sich, dass das Zugangskontrollsystem die Verwendung von Verschlüsselung und mehrstufiger Authentifizierung umfasst. Dies schützt die Kommunikation zwischen Geräten, Steuerungen und mobilen Geräten und stellt sicher, dass es keine Hintertüren für „Wartungszwecke“ gibt.
3. Richten Sie ein unabhängiges Netzwerk ein, das ausschließlich für Geräte bestimmt ist, die mit sensiblen Informationen umgehen, und stellen Sie sicher, dass die Kommunikation zwischen diesen Geräten verschlüsselt ist. Platzieren Sie diese Geräte in einem separaten virtuellen LAN (VLAN) und stellen Sie sicher, dass die Hersteller der installierten Geräte oder Software standardmäßig Implementierungsprotokolle wie HTTPS, TLS, SIPS oder SRTP verwenden.
4. Erstellen Sie verschiedene Konten mit unterschiedlichen Berechtigungen. Auf diese Weise wird sichergestellt, dass die Benutzer nur Änderungen vornehmen können, die mit ihren spezifischen Aufgaben zusammenhängen, während der Administrator größere Rechte erhält, um das Gebäude und alle damit verbundenen Konten zu verwalten.
5. Aktualisieren Sie die Software regelmäßig. Die Installation der neuesten Firmware-Version auf den Geräten ist wichtig, um Cybersecurity-Risiken zu minimieren. Mit jeder neuen Version werden Fehler in der Software behoben und die neuesten Sicherheitspatches implementiert.
6. Schulen Sie Ihre Mitarbeiter, um Social Engineering-Bedrohungen zu vermeiden. Das menschliche Element ist der verwundbarste Teil eines jeden Systems, und Angreifer können Menschen dazu verleiten, Sicherheitsfehler zu begehen oder sensible Informationen preiszugeben. Daher ist es notwendig, die Mitarbeiter regelmäßig zu schulen und in ihr Bewusstsein für Cybersicherheit zu investieren.