UIMCommunic@tion

03/2019

Ausgabe für Deutschland

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Backups sind gut, ein funktionierendes ISMS besser

Der norwegische Aluminiumhersteller Norsk Hydro ist Mitte März Opfer eines massiven Hackerangriffs mit gravierenden Folgen geworden: Die Aktie verlor über 3 Prozent an Wert und konnte den Verlust trotz Schwankungen bisher nicht wieder ausgleichen, die Produktion wurde massiv gestört. Das Problem ist laut Vorstand Eivind Kallevik bisher nicht abschließend behoben worden. Für den erfahrenen IT-Sicherheits- und Datenschutzexperten Dr. Jörn Voßbein ist der Fall ein Weckruf mit vielen Fragen für Unternehmen: „Ist das eigene Unternehmen optimal geschützt vor solchen kriminellen Cyber-Attacken? Was kann und muss in Unternehmen verbessert werden?“ Der Fall aus Norwegen erfordert eine genaue Betrachtung, um die richtigen Lehren zu ziehen.

Das betroffene Unternehmen Norsk Hydro ASA ist ein Unternehmen, das sich auf die Produktion von Aluminium spezialisiert hat. Mit Vertriebs- und Handelsaktivitäten entlang der gesamten Wertschöpfungskette ist der Konzern in über 50 Ländern weltweit aktiv. Über 36.000 Menschen sind bei Norsk Hydro beschäftigt.

Was war passiert? Den norwegischen Sicherheitsbehörden zufolge nutzten die Angreifer den Computervirus LockerGoga. Dieser verschlüsselt die Daten auf den Festplatten der angegriffenen Rechner, so dass kein Zugriff mehr besteht. Das notwendige Passwort für den Zugang zu ihren Daten erhalten die Opfer solcher sogenannter Ransomware meist erst nach einer Lösegeld-Zahlung (doch selbst bei Zahlung ist dies nicht sicher). Norsk Hydro musste teilweise die Produktion stoppen oder auf manuellen Betrieb umstellen. Das gesamte Ausmaß des Vorfalls ist nicht absehbar.

Wie kann man solchen Attacken vorbeugen? Tatsächlich können Unternehmen schon heute viel für die Datensicherheit tun und somit Prävention gegen Cyber-Kriminalität leisten. Der Aufbau eines Informationssicherheits-Managements ist ein wichtiger Baustein zu einer deutlich verbesserten IT-Sicherheit im Unternehmen. Dieses Vorgehensmodell kann sich an den gängigen Normen zum Informationssicherheits-Managementsystem (ISO/IEC 27001 und 27002) orientieren und ist seit Jahren aufgrund seiner Praktikabilität anerkannt. Im Ergebnis entsteht ein Managementsystem, durch das sichergestellt werden kann, dass die Informationssicherheit im Unternehmen gelebt wird, dass sie auf die Bedürfnisse des Unternehmens angepasst ist und dass alle wichtigen Aspekte erfasst werden.

Was kann ich als Sofortmaßnahme tun? Ein in letzter Zeit immer wichtiger werdender Bereich ist die Schulung und Sensibilisierung der eigenen Belegschaft für das Thema IT-Sicherheit und der richtige Umgang mit ihr. Die Erfahrung zeigt, dass Vorgaben nur eingehalten werden, wenn die Mitarbeiter die Hintergründe verstehen. Andernfalls werden entweder bewusst Regeln umgangen, weil sie als „lästig“/unsinnig empfunden werden, oder es wird unbewusst aus mangelndem Wissen gegen Vorgaben verstoßen.

Der Fall Norsk Hydro werde hoffentlich eine Diskussion über die eigenen IT-Sicherheitsmaßnahmen in Gang setzen, an deren Ende dann Verbesserungen auch wirklich vorgenommen werden, so UIMC-Geschäftsführer Dr. Jörn Voßbein. „Nur darüber reden, bringt nichts und erleichtert den Cyber-Kriminellen ihr schmutziges Handwerk weiter zu betreiben – es müssen Taten folgen“, fordert Dr. Voßbein ein höheres Maß an IT-Sicherheit in Unternehmen, „was nicht nur börsennotierte Konzerne, sondern auch für den Mittelstand/für KMU gilt.“

Vorsicht bei E-Mail-Bewerbungen!

Derzeit kursieren wieder gefakte Bewerbungen im Internet. Nach dem Öffnen des Dateianhangs verschlüsselt ein Schädling Daten und fordert Lösegeld.

Daher sollten Sie unbedingt Ihre Mitarbeiter informieren: Die Mail sollte umgehend gelöscht oder (insbesondere, wenn der betreffende Empfänger im Personalbereich ansässig ist) die IT zu Rate gezogen werden. **Unter keinen Umständen sollte der Dateianhang geöffnet werden.**

UIMC® | in Datenschutz und Informationssicherheit stets gut beraten!

UIMC Dr. Vossbein GmbH & Co KG, Otto-Hausmann-Ring 113, 42115 Wuppertal

Tel.: +49-202-946 7726 200, Fax: - 19, E-Mail: consultants@uimc.de, Internet: www.UIMC.de

Noch Fragen?
Treten Sie mit uns in einen Dialog ein!

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Cold Calling: Unter welchen Voraussetzungen darf zur Kaltakquise das Telefon genutzt werden?

Grundsätzlich gilt Analoges zur E-Mail-Werbung: Grundsätzlich ist eine explizite Einwilligung erforderlich. Hierbei gelten die im Rahmen des Datenschutzes genannten Anforderungen an eine Einwilligung ebenfalls. Ausnahmen sind in § 7 UWG explizit zu entnehmen.

Eine Unterscheidung zwischen B2C (Anruf von Verbrauchern) und B2B (Anruf von Unternehmen) ist hierbei sinnvollerweise vorzunehmen:

B2C: Endverbraucher-Ansprache

Private Neukunden dürfen Sie nur dann per Telefon, Fax oder E-Mail kontaktieren, wenn diese Ihnen das ausdrücklich erlaubt haben. Unaufgeforderte Werbeanrufe sind verboten. Die Nachweispflicht trägt der Werbende.

B2B: Geschäftskunden-Kontakte

Grundsätzlich ist Kaltakquise über Anrufe zwar auch im B2B-Bereich nicht erlaubt. Doch im Vergleich zum B2C-Bereich, gibt es eine Ausnahme hinsichtlich der telefonischen Kontakte. Hier reicht schon ein konkludentes Einverständnis aus (§ 7 Abs. 2 Nr. 2 UWG: „Eine unzumutbare Belästigung ist stets anzunehmen (…) bei Werbung mit einem Telefonanruf gegenüber einem Verbraucher ohne dessen vorherige ausdrückliche Einwilligung oder gegenüber einem sonstigen Marktteilnehmer ohne dessen zumindest mutmaßliche Einwilligung (…)“.

IT-Sicherheitskongress

Auch in diesem Jahr wird die UIMCert auf dem 16. IT-Sicherheitskongress in Bonn-Bad Godesberg vor Ort sein. Unter dem Motto

„Wir haben den Normen-Zoo im Griff“

präsentiert die UIMCert Ihre Angebote der Auditierung, Testierung und Zertifizierung innerhalb des umfassenden Zoos von Sicherheits-, Datenschutznormen. Seien Sie dabei und diskutieren Sie mit uns vor Ort.

Bonn, 21.-23. Mai 2019

UIMC bildet aus.

Die Vorteile einer Ausbildung werden viel zu wenig beleuchtet, dabei sind sie glasklar: direkter Einstieg ins Berufsleben, finanzielle Unabhängigkeit, nach erfolgreicher Ausbildung gute Chancen auf einen sicheren Arbeitsplatz und letztlich verbessert eine Ausbildung die Chancen auf dem Arbeitsmarkt:

- Informatik-Kaufleute
- Kaufleute für Büromanagement
- Kaufleute für Marketingkommunikation

mehr unter https://jobs.uimc.de

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

- ☐ Backups sind gut, ein funktionierendes ISMS besser
- ☐ Bösartige E-Mail-Bewerbungen
- ☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu!

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 946 7726 9200 oder formlos per Mail an communication@uimc.de

Mehr Informationen, Hinweise und Tipps finden Sie hier: https://communication.UIMC.de