UIMCommunic@tion
praxisnah.gut.informiert.

06/2022

Ausgabe für Deutschland

Angriffe, Social Engineering und andere Gefahren

Cybersicherheit in Kriegszeiten erfordert Wachsamkeit

Der Verfassungsschutz hat aktualisierte Warnungen vor russischen Cyberangriffen herausgegeben. Die Ukraine-Krieg hinterlässt tiefe Spuren in vielen Sektoren. Die finanziellen Folgen sind an der Tankstelle und im Supermarkt für jedermann zu spüren. Deutschland unterstützt die Ukraine aktiv in ihrem Abwehrkampf gegen Russland. Waren es erst Helme und Panzerabwehrwaffen, sind es nun auch Panzerhaubitzen, die an die ukrainische Armee geliefert werden. Außerdem werden ukrainische Soldaten in Deutschland ausgebildet. Die Bundesrepublik ist damit gemäß dem Völkerrecht zwar nicht Kriegspartei, aber doch klar an der Seite der Ukraine positioniert. Ein moderner Krieg wird auf vielen Schlachtfeldern geführt. „Vor dem Hintergrund des Krieges wird auch im Netz gekämpft. Die Bedrohungslage für deutsche Unternehmen und Behörden ist höchst angespannt", berichtet der Fachmann für Informationssicherheit Dr. Jörn Voßbein. Bestätigt wird diese Ansicht auch durch die aktuellen Sicherheitshinweise des Verfassungsschutzes.

„Vor dem Hintergrund der politischen Lage" sei mit Angriffen auf deutsche Webseiten zu rechnen – so hat das Bundesamt für Verfassungsschutz die Unternehmen und Behörden gewarnt. Konkret wird vor Attacken der prorussischen Hacker-Gruppierung „Killnet" gewarnt. In den vergangenen Wochen waren die pro-russischen Aktivisten offenbar mit einigen Angriffen gegen die Websites deutscher Behörden erfolgreich. Die Seiten des Bundeskriminalamtes (BKA) und der Bundespolizei waren offenbar bereits Ziele von massenhaften, koordinierten Störversuchen. Laut einem internen Behördenbericht waren auch die Web-Präsenzen des Bundestags, des Bundesverteidigungsministeriums und die SPD-Website von Bundeskanzler Olaf Scholz Ziel von Attacken.

Das klingt erstmal bedrohlich. Die offenbar Putin-treuen Hacker führten aktuell „eine Kampagne gegen diverse deutsche Webseiten aus Privatwirtschaft und Forschung", heißt es im Sicherheitshinweis des deutschen Inlandsgeheimdienstes. Gewarnt wird insbesondere vor sogenannten DDoS-Angriffen, die zum Ziel haben, Websites durch massenhafte künstliche Aufrufe lahmzulegen. Nebenbei warnt das Amt auch vor der Ransomware-Gruppierung „Revil". Die Gruppe erpresst ihre Opfer, nachdem sie deren Systeme lahmgelegt hat.

Doch neben den o. g. Angriffsszenarien kommt dem Social Engineering eine immer stärkere Bedeutung zu. Hierbei handelt es sich um Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen oder zum Klicken eines (virenbehafteten) Links zu bewegen.

Dass die Warnungen nicht abstrakt, sondern sehr konkret sind, zeigt auch, was „Killnet" unternimmt. Die „Killnet"-Hacker haben in ihrem Kanal auf dem Messengerdienst Telegram eine Liste mit den Webadressen verschiedener deutscher „Ziele" gepostet – offenbar als Aufruf an ihre Gefolgschaft. Außerdem warnt der Verfassungsschutz russische Staatsangehörige in Deutschland, die in für Russland wichtigen Wirtschafts- und Forschungszweigen arbeiten, vor Anbahnungsversuchen durch russische Nachrichtendienste. Hier bestehe eine erhöhte Gefährdungslage.

Welche Handlungsempfehlungen gibt es in der aktuellen Situation?

Antworten unter www.uimc.de/news

Mehr Informationen zur Cybersicherheit/Informationssicherheit

Innerhalb unserer web.eCollege-Seminare erhalten Sie wichtigen Input zu verschiedenen Themen der Informationssicherheit und zum Datenschutz. Melden Sie sich kostenfrei an: www.uimc.de/webecollege. Sie haben interessante Seminare verpasst? Kein Problem: Dann schauen Sie auf Rückseite der heutigen UIMCommunikation-Ausgabe.

UIMC | nachhaltig.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?
Wir freuen uns über Ihren Anruf!
+49 202 946 7726 200

UIMCommunication
praxisnah.gut.informiert.

UWG: Absurde Rechtsprechung, die aber beachtet werden sollte

Werbung per E-Mail darf gemäß dem Gesetz gegen unerlaubten Wettbewerb (UWG) nur mit ausdrücklicher Einwilligung des Adressaten verschickt werden. Das Kammergericht Berlin hat in einem Urteil vom September 2021 noch einmal unterstrichen, wie eng diese Regelung auszulegen ist.

‚XXXX. Organisiert, denkt mit, erledigt. – Nutzen Sie www.XXXX.de'

so lautete es im Footer, also im untersten Abschnitt einer E-Mail, die ein Unternehmen verschickt hatte. Die Mail an sich hatte einen ganz anderen, nicht aus Werbung bestehenden Sachbezug. Aber die letzten acht Worte hatten es in sich: Der Empfänger sah darin unerlaubte Werbung per elektronischer Post gemäß dem Gesetz gegen den unlauteren Wettbewerb (UWG) und klagte vor dem Kammergericht Berlin.

Das beklagte Unternehmen brachte dagegen vor, dass der Text nur einen Bruchteil der Mail ausmache, getrennt am Ende der Nachricht ist und nicht im Zusammenhang mit dem Rest der Mails stehe. Außerdem seien keine Anhänge mitversendet worden und damit die beanspruchte Speicherkapazität auf ein Minimum beschränkt gewesen. All das half aber nicht. Das Kammergericht wägte die Argumente zu Lasten des beklagten Unternehmens ab.

Zuletzt hatte der Bundesgerichtshof im Jahr 2018 das Werbeverbot sehr eng ausgelegt und dieser Entscheidung folgte nun das Kammergericht. Das Hinzufügen von Werbung zu einer ansonsten zulässigen Mail ist – zumindest nach Ansicht des BGH – keine solche Bagatelle, dass eine Belästigung ausgeschlossen wäre. Der Empfänger der Mail müsse sich zumindest gedanklich mit den werblichen Elementen beschäftigen. Der BGH sah vor allem das Risiko, dass die für sich genommen geringfügige Belästigung zu Nachahmungseffekten von anderen Unternehmen führe und letztlich in Summe zu einer erheblichen Beeinträchtigung der Interessen der Mail-Empfänger werde. Es müsse die Möglichkeit gegeben werden, der Verwendung der Mail-Adresse zum Zwecke der Werbung zu widersprechen.

Gesamter Artikel unter www.uimc.de/news

UIMC vor Ort:

23.06.2022: Tag der IT-Sicherheit | Mannheim
06.07.2022: Cybersecurity Day | Saarbrücken
28./29.09.2022: Fachmesse Krankenhaus Technologie | Gelsenkirchen
25.-27.10.2022: it'sa | Nürnberg

Wir freuen uns auf Ihren Besuch!

web.eCollege
kompakt praxisnah informieren

Sie haben das letzte web.eCollege verpasst, würden aber gerne noch mehr zum den vergangenen Themen erfahren? Dann schauen Sie sich die Unterlagen und/oder die Aufzeichnung an:

http://update.uimcollege.de

Sie können sich als Gast anmelden. Hierzu geben Sie bitte den Code ein, den Sie bei uns erfragen können.
Sofern Sie als Kunde bereits Zugangsdaten für einen anderen Kurs im eCollege haben, können Sie sich auch „selbst einschreiben". Die Einschreibung bleibt einen Monat bestehen.

Die nächsten Termine [kostenfrei]

13.07.2022: 7 nützliche Tipps für eine Lieferantenbewertung / Dienstleister-Auditierung

10.08.2022: 5 Anforderungen beim Drittlandtransfer

14.09.2022: Compliance in KMU: Datenschutz, Informationssicherheit u. ä.

Anmeldung unter www.uimc.de/webecollege

Aktuelles im Online-Formular-Center

» alle Unterlagen sind aktuell

Um über Neuerungen zeitnah informiert zu werden, können Sie künftig unser News-Forum abonnieren und erhalten daraufhin eine E-Mail (siehe oben).

www.uimcollege.de

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

Einer künftigen Zusendung können Sie jederzeit formlos per E-Mail an communication@uimc.de widersprechen.