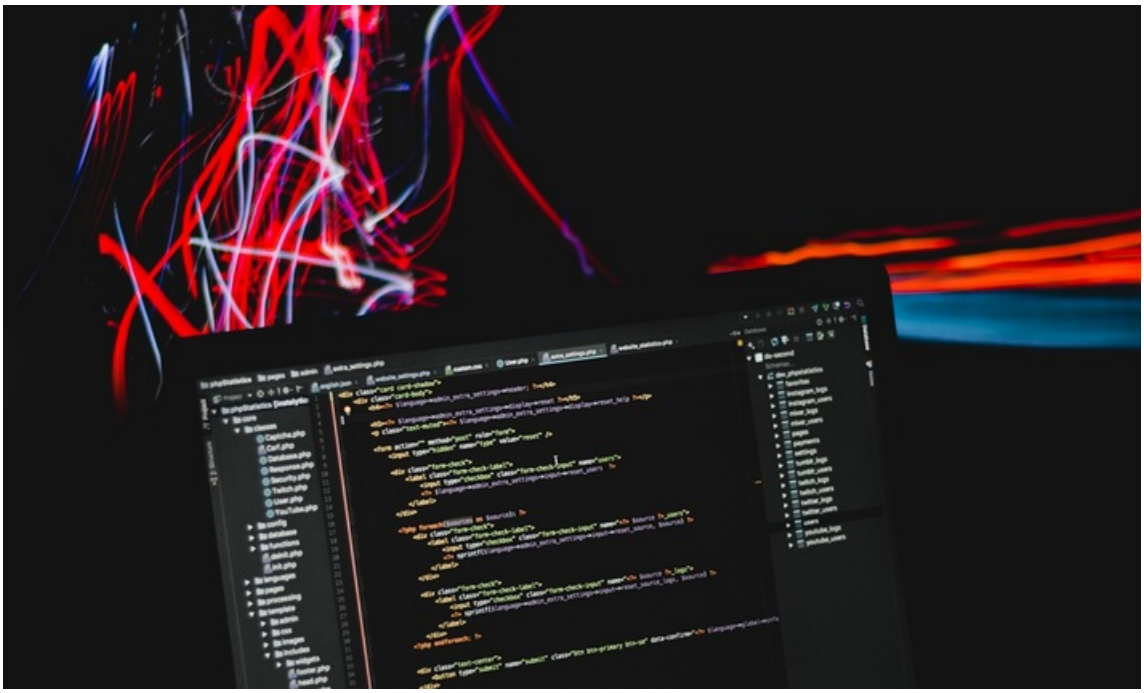
na•news aktuell
Ein Unternehmen der dpa-Gruppe

news aktuell (Schweiz) AG

13.02.2020 – 15:25 Uhr

BLOGPOST Cyberkriminalität: "Irgendwann wird es jeden treffen"



Cyberangriffe können immensen Schaden anrichten. Dabei stellt sich gar nicht mehr die Frage, ob sie ein Unternehmen treffen, sondern wann sie es tun. Seit gestern tauschen sich Cyber-Security-Experten, Unternehmensvertreter und Behörden auf den Swiss Cyber Security Days(SCSD) über die jüngsten Gefahren und mögliche Prävention aus. Wir haben die Mitorganisatoren Milena Thalmann (Head of Business Development) und Nicolas Mayencourt(Head of the Program Comission) gefragt, was Unternehmen gegen Cyberkriminalität tun können und welche Gefahr manipulierte Informationen und Social Bots für die Demokratie bedeuten.

news aktuell: Cyberkriminalität hat viele Facetten. Können Sie uns einen kurzen Einblick in die wichtigsten Tätigkeitsfelder von Internetkriminalität nennen?

Mayencourt: Cyberkriminalität gehört zu den lukrativsten und grössten Geschäften unserer Zeit. Der kriminelle Zweig des Internets ist geschätzte 1.5 Trillionen US-Dollar schwer - im Vergleich dazu: die zehn grössten Internet-Companies zusammen sind gerade mal 750 Milliarden US-Dollar wert.

Zur besseren Einordnung der Tätigkeitsfelder unterscheiden wir zum einen die verschiedenen Akteure einer Attacke (organisierte Kriminelle, staatliche Akteure, Hacktivisten und Privatpersonen). Zum anderen betrachten wir das Ziel einer Attacke (Privatpersonen, Unternehmen, Staaten oder Interessensgruppen). Cyber-Attacken können sodann verschiedene Formen haben, etwa Datendiebstahl, Datenmissbrauch, Infizierung via Viren, Malware etc., Daten-Verschlüsselung (mit Ziel der Erpressung), Spionage oder Verhaltensmanipulation (etwa in der Politik oder beim Kaufverhalten).

Wichtig für eine Einordnung der Attacke ist auch die Analyse der betroffenen Daten. Handelt es sich um persönliche Daten, Zugangsdaten, vertrauliche Daten, statistische Daten oder gar um gefälschte Daten?

news aktuell: Wie hat sich Cyberkriminalität in der Schweiz in den letzten fünf Jahren entwickelt?

Mayencourt: Einen fundierten Überblick gibt die Statistik von Fedpol. Dieser Bericht zeigt vor allem eins: Die Zahl der Verdachtsmeldungen ist massiv zurückgegangen. Möglicherweise liegt das daran, dass Nutzer besser informiert sind und mehr relevante Meldungen absetzen. Oder, dass Angriffe besser getarnt und weniger offensichtlich zu entdecken sind. Vielleicht nimmt aber auch die Angst vor Strafen zu, oder die Angriffe werden weniger, weil sie immer lukrativer werden. Hinter den Zahlen stecken viele Mutmassungen.

news aktuell: Was können Unternehmen konkret tun, um sich vor Cyberangriffen zu schützen?

Thalmann: Cyberkriminalität muss gesamtgesellschaftlich als reale Bedrohungslage anerkannt werden. Wie die

Eltern ihren Kindern beibringen, für einen Lolli nicht mit Fremden mitzugehen oder mittlerweile auch Regeln für die Mediennutzung vermitteln, müssen erst recht Erwachsene lernen, ihre Daten nicht für eine bequeme Funktion in einer App preiszugeben. Das gilt für Privatpersonen wie für Unternehmen. Letztere sollten jetzt breite Handlungsfelder aufbauen. Die Digitalisierung ist weiter, als uns die Medien glauben lassen. Schon heute sind zahlreiche Systeme firmenintern und -extern verbunden. Dies bedarf komplexen Schutzmechanismen, die sowohl technisch als auch prozessual konzipiert werden müssen.

Mayencourt: Cybersicherheit ist keine Disziplin der IT-Abteilung. Der Versuch, dies hier zu lösen, sollte aktuell als gescheitert betrachtet werden. Geschäftsführungen müssen über Sicherheitsparameter informiert sein, C-Level braucht Prioritäten und operative Teams müssen die Sicherheit als fixen Bestandteil ihrer Projekte sehen.

Thalmann: Zudem gilt es, Mitarbeiter zu schützen und zu stärken. Dazu gehört Wissensvermittlung, Training und auch Visibilität. Unternehmen sollten ihre Assets nicht nur schützen, sondern auch aus einer Varianz an Perspektiven in Echtzeit beobachten. Zudem müssen Unternehmen den Mitarbeitern Freiraum geben, sich dem Thema Datenschutz zu widmen. Lieber eine Mail zweimal lesen, als eine vorschnelle Handlung befürworten.

Mayencourt: Unternehmen müssen Verantwortung übernehmen. Sie müssen ihre Produkte (physisch wie digital) in ihren Bestandteilen sicher machen, bevor sie sie in den Markt einführen. Damit vermeiden Unternehmen, Käufer und Nutzer in Gefahr zu bringen.

news aktuell: Und was tun, wenn ein Schaden passiert ist?

Thalmann: Saubere Backups mit Medienbruch schützen vor Erpressung. Saubere Kommunikation schützt ein Unternehmen vor Reputationsschaden. Und saubere Analyse des Vorfalls schützt vor Folgeschäden.

news aktuell: Welchen Stellenwert sollte Cybersecurity in der professionellen Kommunikation haben?

Thalmann: Die Frage, die sich jede Branche stellen muss, ist: Was schütze ich? Bei PR-Agenturen betrifft das zum Beispiel Kundendaten, Kampagnenmaterial und Branchengeheimnisse, da Agenturen oft vertrauliche Daten von Kunden vor deren Veröffentlichung handhaben.

Zudem können Kommunikationsabteilungen in Unternehmen viel tun hinsichtlich Prävention, Aufklärung und Firmenkultur. Es gibt Unternehmen, die ohne aktuellen Bezug ihre Mitarbeiter und Kunden regelmässig über Veränderungen und Herausforderungen in Sachen Cybersecurity informieren. Ohne dabei belehrend zu sein. Es geht um ein wachsendes Bewusstsein und Transparenz im Unternehmen.

Mayencourt: Zukünftig werden auch Fake News, die etwa durch Bots oder Trolls generiert und verbreitet werden, eine grosse Rolle spielen. Daher müssen Kommunikationsexperten ein grosses Spektrum an Plattformen monitoren und sich Wissen über entsprechende Reaktionen aneignen. Aktuell erfolgt hier oft eine Zensur durch schnelles Löschen, dies kann unter Umständen zu einer unkontrollierten Gegenreaktion führen. Immer noch wird das Problem in Unternehmen in der Praxis oft nur mit technischen Lösungen (hier Firewall, da Anti-Virus Software) angegangen und führt dabei direkt an der Unternehmenskommunikation vorbei.

news aktuell: Sollten Unternehmen Cyberkriminalität in ihr Krisenmanagement integrieren?

Mayencourt: Unbedingt. Es kann jeden treffen. Jederzeit. Es gibt drei verschiedene Typen von Unternehmen: 1) die, die schon gehackt wurden, 2) die, die noch gehackt werden und 3) die, die es nicht merken. Alle werden ein Security Vorfall erleben, die Frage ist nicht ob, sondern wann. Es wäre also besser, vorbereitet zu sein.

news aktuell: Welche Fehler sollten Unternehmen bei der Kommunikation während einer akuten Krisensituation, die durch Cyberkriminalität entstanden ist, unbedingt vermeiden?

Mayencourt: Sie sollten keinesfalls Schuldzuweisungen machen a la "Das war dieser Mitarbeiter oder diese Abteilung, die den Fehler begangen hat". Ein weiteres No Go: die Folgen vertuschen.

news aktuell: Wie ordnen Sie im Kontext von Cyberkriminalität die Zunahme von manipulierten Informationen und Social Bots ein?

Thalmann: Bots und Botnets gehören zur Cyberkriminalität und nehmen einen wichtigen Stellenwert ein. Irreführung, Manipulation und Fälschung des Verrechnungssystems (wer profitiert von was) sind nur die offensichtlichen Folgen eines Bot-Einsatzes. Ins Gewicht fällt vor allem der Einsatz von Bots im Zusammenhang mit politischen Systemen.

Mayencourt: Meinungslenkung und -bildung durch Technologien sind in den USA, Israel, Russland oder China schon sehr weit fortgeschritten. Die Auswirkungen auf die Marktbeeinflussung sind noch unerforscht, aber bei genauem Hinsehen sichtbar.

news aktuell: Wie gefährlich schätzen Sie die Wirkung von Social Bots für Bots für die öffentliche Meinungsbildung und demokratische Prozesse ein?

Mayencourt: Je weiter unsere Gesellschaft sich ihre Meinung via Empfehlungsforen und sozialen Plattformen bildet, desto gefährlicher wird es. Wir haben verlernt, Informationen auf ihren Urheber und ihren Wahrheitsgehalt zu prüfen. Wir lesen mehr Headlines als tatsächliche Berichtserstattungen. Digitale Personas beeinflussen, was wir gut und schlecht finden, Algorithmus beeinflusst, was wir zu sehen bekommen. Und dies ist bei vielen, auch kommerziellen Akteuren schon salonfähig. Wenn dieses Verhalten manipuliert wird und ein Algorithmus unsere Bedürfnisse mit seinen Zielen verknüpft und über Bots ausspielt, beginnen wir von Propaganda zu sprechen.

news aktuell: Deep Fakes werden immer ausgetüftelter. Wie schätzen Sie die Entwicklung diesbezüglich in den kommenden Jahren ein?

Thalmann: Wir müssen wieder Quellen und Urheber prüfen, bevor wir Informationen vertrauen. Diese Entwicklung ist extrem bedenklich. Bild- und Videomanipulation gab es schon immer. Aber die Exzellenz macht es immer schwieriger.

Mayencourt: Wir werden in einer Gesellschaft leben, die Vertrauen neu definieren muss. Aber "Wie?" ist noch völlig unklar. Es wird eine gesamtgesellschaftliche Herausforderung.

news aktuell: Wie können sich Unternehmen, aber auch Parteien und Institutionen Ihrer Meinung nach vor Falschinformationen und Social Bots schützen?

Thalmann: Mit Hilfe von Monitoring, Analyse und auch mehr Transparenz. Einen guten Schutz gibt es erst, wenn Plattformen sich zu besseren Massnahmen verpflichten. Solange gilt es, gewisse Plattformen mit Vorsicht zu geniessen und etwas weniger freizügig mit den Informationen über die eigene Person umzugehen.

Mayencourt: Wir sollten anfangen, einzufordern, dass alle falschen, gefälschten, manipulierten und irreführenden Inhalte offengelegt werden. Das würde den Nutzern zu mehr Orientierung helfen.

news aktuell: Welche Strukturen müssen geschaffen werden, um hier nachhaltig vorzubeugen und wirksame Gegenmaßnahmen zu etablieren?

Mayencourt: Die Unternehmen müssen Verantwortungen schaffen und übernehmen. Sie müssen mehr Rahmenbedingungen in der Politik fordern, für die Befähigung ihrer Mitarbeiter einstehen und Budget, Zeit sowie Kompetenzen schaffen. Wir als Gesellschaft müssen dafür sorgen, dass das Thema bereits in unserem Bildungssystem verankert wird und alle gleichermassen sensibilisiert sind.

Interview: Beatrix Ta

Nicolas Mayencourt ist IT- und Cybersicherheitsexperte mit 25 Jahren Erfahrung. Er ist damit ein Pionieer als Sicherheitsakteur und ein "Hacker" der ersten Generation. Seine Vision: Cybersicherheit für die Gesellschaft, Wirtschaft und Nationen schaffen. Durch seine Arbeit für relevante Unternehmen und Regierungen auf der ganzen Welt ist er inzwischen einer der gefragtesten Berater. Er und sein Team bei Dreamlab Technologies testen, sichern und machen sichtbar, was in der Cyber-Dimension oft unentdeckt bleibt. Er setzt sich ein für Souveränität, offene Standards, ist Mitautor des OSSTMM, Kontributor in ISO, Mitglied des W3C und arbeitet im Verwaltungsrat mehrerer Unternehmen. Innerhalb der SCSD-Organisation ist er Head of the program commission.

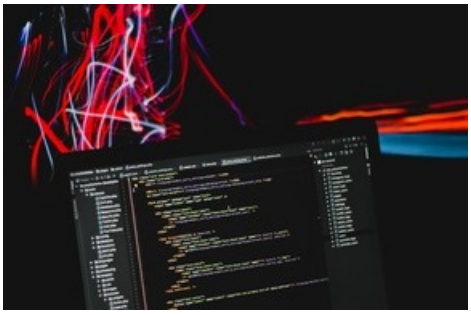
Milena Thalmann ist Marketing- und Kommunikationsexpertin für die IT-Branche. Aktuell arbeitet sie bei Dreamlab Technologies AG. Im Namen der Firma verantwortet sie die Aufklärungsarbeit über Sicherheit und Sicherheitslücken in der Schweiz. Sie ist ausserdem als Head of Business Development für die konzeptionelle Umsetzung der Swiss Cyber Security Days mitverantwortlich.

Dieser Beitrag ist ein Original-Post aus dem news aktuell Blog:

https://www.newsaktuell.ch/blog/cyberkriminalitaet-irgendwann-wird-es-jeden-treffen/

Beim news aktuell-Blog geht es um die Themen Kommunikation, PR, Pressearbeit, Journalismus/Medien, Marketing und Human Resources. Und manchmal auch um news aktuell selbst. Welche Trends, welche Apps, welche Themen bewegen Kommunikations-, Marketing- und HR-Fachleute heute? Wie sieht unser Arbeitstag aus? Was ist wichtig für die Karriere? Damit wollen wir uns beschäftigen. Wir zeigen was die Branche antreibt. In Best Practice, in Interviews oder in Gastbeiträgen.

Medieninhalte



Cyberangriffe können immensen Schaden anrichten. Dabei stellt sich gar nicht mehr die Frage, ob sie ein Unternehmen treffen, sondern wann sie es tun. Seit gestern tauschen sich Cyber-Security-Experten, Unternehmensvertreter und Behörden auf den Swiss Cyber Security Days (SCSD) über die jüngsten Gefahren und mögliche Prävention aus. Wir haben die Mitorganisatoren Milena Thalmann (Head of Business Development) und Nicolas Mayencourt (Head of the Program Comission) gefragt, wie sich Cyberkriminalität in der Schweiz in den letzten Jahren entwickelt hat und was das für die Kommunikationsbranche bedeutet. Foto: fabian grohs / unsplash

Milena Thalmann ist Marketing- und Kommunikationsexpertin für die IT-Branche. Aktuell arbeitet sie bei Dreamlab Technologies AG. Im Namen der Firma verantwortet sie die Aufklärungsarbeit über Sicherheit und Sicherheitslücken in der Schweiz. Sie ist ausserdem als Head of Business Development für die konzeptionelle Umsetzung der Swiss Cyber Security Days mitverantwortlich. Foto: Kevin Zehnder

Nicolas Mayencourt ist IT- und Cybersicherheitsexperte mit 25 Jahren Erfahrung. Er ist damit ein Pionieer als Sicherheitsakteur und ein Hacker der ersten Generation. Seine Vision: Cybersicherheit für die Gesellschaft, Wirtschaft und Nationen schaffen. Durch seine Arbeit für relevante Unternehmen und Regierungen auf der ganzen Welt ist er inzwischen einer der gefragtesten Berater. Er und sein Team bei Dreamlab Technologies testen, sichern und machen sichtbar, was in der Cyber-Dimension oft unentdeckt bleibt. Er setzt sich ein für Souveränität, offene Standards, ist Mitautor des OSSTMM, Kontributor in ISO, Mitglied des W3C und arbeitet im Verwaltungsrat mehrerer Unternehmen. Innerhalb der SCSD-Organisation ist er Head of the program commission.