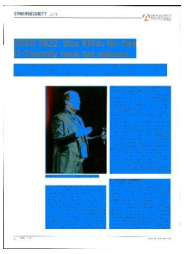
Datum: 12.05.2022

IT-MARKT



L//P

IT-Markt
8005 Zürich
044/ 355 63 63
https://www.it-markt.ch/

Medienart: Print
Medientyp: Fachpresse
Auflage: 4'802
Erscheinungsweise: 8x jährlich

Seite: 24
Fläche: 141'245 mm²

Auftrag: 1093187
Themen-Nr.: 666.014

Referenz: 84267121
Ausschnitt Seite: 1/3

SCSD 2022: Was KMUs für ihre IT-Security noch tun müssen

An den diesjährigen Swiss Cyber Security Days hat das Publikum einen Einblick in die digitale Bedrohungslage erhalten. Bundesrat Ueli Maurer kündigte ein Bundesamt für Cybersicherheit an. Der Cyber-Chef der USA sprach über die Entscheidung zwischen «gut» und «nicht gut». Und die Mobiliar zeigte, wo Nachholbedarf bei KMUs besteht. Autoren: René Jaun und Coen Kaat

Florian Schütz, Delegierter des Bundes für Cybersicherheit.

Im Forum Fribourg haben die diesjährigen Swiss Cyber Security Days (SCSD) stattgefunden. «Heute ist jeder mit jedem verbunden, wie in einem globalen Dorf», sagte Nationalrätin und SCSD-Präsidentin Doris Fiala zu Beginn der Veranstaltung. Nach Erde, Wasser, Luft und Weltraum stelle Cyber somit eine neue, fünfte Dimension dar. Die Wichtigkeit dieser Dimension zeige sich aktuell etwa am Krieg in der Ukraine, der auch digital ausgetragen werde.

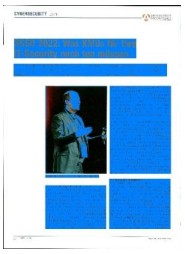
Wie sich der Bund in puncto Cybersecurity engagiert, erklärte Bundesrat Ueli Maurer in einer Videobotschaft. Man sei gemeinsam unterwegs, sagte der Finanzminister, er stellte aber auch klar: «Aus Sicht des Bundes spielen wir hier nur eine sekundäre Rolle», und der Bund wolle die Wirtschaft unterstützen. In der Folge zählte Maurer einige Beispiele der Zusammenarbeit von Bund und Wirtschaft auf. Zu den aktuellen gehört der erst kürzlich gegründete Verein für mehr Cyberresilienz des Schweizer Finanzplatzes, der vom Nationalen Zentrum für Cybersicherheit (NCSC) unterstützt wird. Und das Thema soll für Bundesbern noch wichtiger werden: «Wir beabsichtigen, ein Bundesamt für Cybersicherheit zu formen», gab Maurer bekannt. Dieses solle die Rolle einer zentralen Ansprechstelle übernehmen.

Mehr ins Detail ging danach Florian Schütz, Delegierter des Bundes für Cybersicherheit, auch bekannt als «Mr. Cyber». Er zeigte auf, was sich im Rahmen der nationalen Cybersecurity-Strategie in den vergangenen Jahren bereits getan hat. Erst kürzlich habe das von ihm geleitete NCSC beispielsweise die Website ergänzt: Neu gibt es spezifische Informationen für Behörden und detailliertere Statistiken zu eingegangenen Meldungen. Dank letzteren sollen sich Unternehmen ein Bild der aktuellen Bedrohungslage machen und sich vorbereiten können.

In seinem Ausblick zeigte Schütz einen ersten Entwurf der Cyberstrategie für die kommenden Jahre. Zu deren Zielen gehören unter anderem: Selbstbefähigung, Ahndung der Täter, internationale Zusammenarbeit sowie Sicherheit und Verfügbarkeit kritischer Infrastrukturen sicherstellen.

Datum: 12.05.2022

IT-MARKT



L//P

IT-Markt
8005 Zürich
044/ 355 63 63
https://www.it-markt.ch/

Medienart: Print
Medientyp: Fachpresse
Auflage: 4'802
Erscheinungsweise: 8x jährlich

Seite: 24
Fläche: 141'245 mm²

Auftrag: 1093187
Themen-Nr.: 666.014

Referenz: 84267121
Ausschnitt Seite: 2/3

Die alte Botschaft, neu formuliert

Ein traditioneller Teil der SCSD bildet die Analyse der Cyberbedrohung in der Schweiz. Präsentiert wurde diese von Marc Peter, Leiter des Kompetenzzentrums Digitale Transformation an der FHNW, und Nicolas Mayencourt, Leiter der Programm-Kommission der SCSD. Die gute Nachricht: Nachdem ihr Scan vergangenes Jahr mehr als 113 000 Verwundbarkeiten zutage gefördert habe, seien es diesmal nur noch 106 000 gewesen, erklärte Mayencourt – jedoch noch immer deutlich zu viele. Zudem nehmen die durch Cyberangriffe entstandenen Schäden ein immer grösseres, manchmal existenzbedrohendes Ausmass an.

Die Sensibilisierung in der Bevölkerung für Cyberrisiken habe zwar zugenommen, räumt Mayencourt ein, aber: «Wir alle haben das Gefühl, es betrifft uns nicht, und es kann uns nicht treffen», sagte er im Interview, und berief sich dabei auf eine unlängst durchgeführte Studie.

Mayencourts Botschaft ist nicht neu: «Hören wir auf, naiv zu sein», sagte er. Allerdings wurde er diesmal noch einmal deutlicher: «Wir sind alle das Problem. Wir sind aber auch alle die Lösung. Und darum: Let's make it happen!»

Die gute Cyberstrategie

Ebenfalls eine Keynote hielt Chris Inglis, National Cyber Director der USA und persönlicher Berater des US-Präsidenten Joe Biden. «Die Schweiz ist die Nummer eins in Innovation», lobte er und fügte an: «Sie sind im Moment vielleicht nicht die Nummer eins in Cyber, aber ich glaube, Sie sind dabei, dies zu ändern.» Cybersicherheit sei eine internationale Angelegenheit und erfordere eine gemeinsame Antwort. Gefragt, welche Cybergefahr er als die grösste einstufe, sagte Inglis: «Was mich nachts wachhält, ist in erster Linie keine der Bedrohungen, die wir haben, auch wenn es davon viele gibt. Es ist die vorsätzliche Uneinsichtigkeit, die ich bei so vielen sehe.» Jedes Unternehmen habe die Wahl, sich zwischen «gut» und «nicht gut» zu entscheiden. Inglis schloss mit einem positiven Gedanken: «Wir können die massiven Rechenkapazitäten des World Wide Web nutzen, um gute Dinge zu tun. Ich will aufhören, mich vom Gedanken an Gefahren leiten zu lassen. Ich behalte sie im Auge, aber ich will darüber nachdenken, wo ich hinwill.»

Der zweite Tag startete mit einer Rede von Gerhard Andrey, Nationalrat und Mitgründer von Liip. In seiner Keynote ging er darauf ein, wie die Luftfahrtindustrie auf technische Defekte in komplexen Systemen mit einer transparenten Sicherheitskultur reagiere. «Von dieser Kultur sollte sich die gesamte Digitalbranche eine Scheibe abschneiden», sagte er. Auch im Umgang mit Cybersecurity-Themen sollte eine präzise und vollständige Informationsübermittlung zum Standard werden. Ferner sprach er auch über das Thema Open Source. Zu viele würden davon profitieren – zu wenige dazu beitragen. «Es muss zu einer Selbstverständlichkeit der Branche werden, solche Ansätze zu unterstützen», forderte er.

Es hapert bei der Organisation, nicht an der Technik

Anschliessend gab die Versicherungsgesellschaft Mobiliar einen Einblick in zwei Studien. Diese ergaben, dass die Schweizer KMUs bei den technischen Massnahmen gut aufgestellt seien. So würden 90 Prozent der Befragten regelmässige Software-Updates einspielen, 86 Prozent ihr WLAN mit Passwörtern sichern und 84 Prozent eine Firewall einsetzen, heisst es in der Studie. Bei den organisatorischen Massnahmen «sieht das Bild bedeutend anders aus», sagte Andreas Hölzli, Leiter Kompetenzzentrum Cyber Risk. Nur 77 Prozent prüfen gemäss der Studie, ob sie ihre Daten aus den Backups wiederherstellen können. Einen Notfallplan haben 58 Prozent und regelmässige Mitarbeiterschulungen führen nur 39 Prozent der Befragten durch. Ein Notfallplan sei aber wichtig. So könne man die Reaktionsfähigkeit in einer Notlage gewährleisten. Der Plan soll klar regeln, wer für was zuständig ist, wie man diese Personen erreicht und das Vorgehen im Ernstfall Schritt für Schritt definieren. «Ich würde den Notfallplan aber auf Papier schreiben oder ihn wenigstens ausdrucken», sagte Hölzli. Denn im Falle eines Angriffs könnte er andernfalls nicht zugänglich sein.

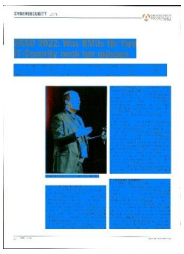
Die nächste Ausgabe der Swiss Cyber Security Days wird am 29. und 30. März 2023 stattfinden.

Datum: 12.05.2022

IT-MARKT

IT-Markt
8005 Zürich
044/ 355 63 63
https://www.it-markt.ch/

Medienart: Print
Medientyp: Fachpresse
Auflage: 4'802
Erscheinungsweise: 8x jährlich



Seite: 24
Fläche: 141'245 mm²

Auftrag: 1093187
Themen-Nr.: 666.014

Referenz: 84267121
Ausschnitt Seite: 3/3

Nicolas Mayencourt, Leiter der Programm-Kommission der SCSD.

Doris Fiala, Nationalrätin und SCSD-Präsidentin.