

November 2017: PRESENTATIE INTERNETBEVEILIGING

Een beveiligingsexpert lichtte clubleden en invit es voor over de gevolgen van criminele hacking van internetaansluitingen. Nieuwe wetgeving voor het beheren van eigen aansluitingen wordt van kracht medio 2018; wat dit voor een ieder betekent en hoe de risico's af te dekken werd helder uiteengezet.



Christian von G ler sprach im PAN auf Einladung des Lions Clubs Montferland-Emmerich.

FOTO: THORSTEN LINDSAMP

Daten sind das Gold von morgen

Christian von G ler aus D sseldorf referierte bei den Lions Montferland-Emmerich  ber Cyber Attacken. Auch im Hinblick auf neue EU-Datenschutzgrundverordnung

Von Dirk Kraaywinger

Emmerich. Eindrucksvoll, die Online-Angriffe, die Christian von G ler am Dienstagabend den Besuchern der Vortragsveranstaltung des Lions-Clubs Montferland-Emmerich im PAN pr sentierte. Bei der Telekom und deren Partner gab es weltweit in einer Minute 891 solcher Cyber-Attacken, mehr als 117.000 waren es in einer Stunde. Der Fachmann der Best-Gruppe D sseldorf, die sich auf Versicherungsmakeln spezialisiert hat, sensibilisierte das Publikum, worauf ein Unternehmer achten muss, wenn's um die Daten im Netz geht.

Kein Unternehmen ist zu klein

Als er eingangs die Frage stellte, wer denn ein Smartphone habe, so zeigten bis auf einen alle auf. Mit Blick auf Freddy Heinzl - ohne Smartphone - erkl rte von G ler: „Er lebt sicherer.“ Ob Webcam oder Drucker - alles Dinge, die Daten an Unberechtigte gelangen lassen. „Innerhalb von zwei Jahren ist dieses Unternehmensrisiko von

PERS NLICHE E-MAIL-ADRESSE  BERPR FEN LASSEN

■ **Kriminelle** versuchen, sich mit E-Mail-Adressen und den zugeh rigen Passw rtern in E-Mail-Konten, Online-Dienste oder Internet-Foren einzuloggen. Das Bundesamt f r Sicherheit in der

Informationstechnik (BSI) bietet hierzu einen Check an. Auf der Homepage www.sicherheits-test.bsi.de kann man seine pers nliche E-Mail-Adresse  berpr fen lassen. DK

Platz 6 auf 1 gestiegen“, w sste er. Schnell widerlegte der Mann aus der Landeshauptstadt, dass solche Argumente, wie „Unser Unternehmen ist zu klein“, „Wir haben eine Top-IT“ oder wir „Vertrauen unseren Mitarbeitern“ ein Trugschluss seien. Gerade die Gefahr von innen sei am gr o ten: „Vielfach werden aktuelle und ehemalige Mitarbeiter zu T tern.“ Dagegen sind die einst f hrenden Hobby-Hacker auf die unteren R nge abgerutscht.

Noch eines wusste Christian von G ler: „IP-Adressen, die man von au en erreichen kann, sind ganz gef hrlich.“ Alles was au erhalb des Unternehmens zug nglich ist,

wie etwa IP-Adressen von Druckern, b te viel Energie f r kriminelle Machenschaften.

 ber die Suchmaschine Shodan lie en sich mit dem Netz verbundene Webcams, Router, Server und eben Drucker, PC-Arten und Dienste finden. Wenn eine Attacke einmal begonnen habe „sind die Viren in der Tiefe der Betriebssysteme zu finden“.  hnlich sei es auch bei der Klinik in Neuss gewesen. Mit der virtuellen W hrung Bitcoins k nnte man die Daten wieder zug nglich machen. W hrend in den USA das FBI dazu rate, wirtschaftlich abzuw gen, ob man L segeld zahle, werde in Deutschland

davon abgeraten. Man wisse ja nicht, ob auch tats chlich die Datenfreigabe erfolge.

Auf die ab Mai 2018 in Kraft tretende EU-Datenschutzgrundverordnung ging der Experte ebenfalls ein. Unternehmen w rden mangelhaft aufgekl rt. Zudem w rden derzeit nur zehn Prozent der Firmen diese umsetzen. „Ab n chstes Jahr wird's teuer, wenn man ab zehn Personen keinen Datenschutzbeauftragten hat.“

Ein Notfallkonzept, umfangreiche Dokumentationen, eine Cyber-Versicherung, Penetration Tests, bei denen gezielt Viren, Trojaner und E-Mails die Systeme befallen w rden, seien ein gutes Mittel. Mitarbeiter solle man ermuntern sich zu melden, wenn diese eine verd chtige E-Mail ge ffnet haben. Christian von G ler r t zur t glichen Datensicherung au erhalb des Firmenservers. Sicherungsdauer: acht Wochen. „Daten sind das Geld von morgen und haben schon lange das  l  berholt.“ Der Umsatz sei gr o er als der des weltweiten Drogenhandels.