RISIKOFAKTOR MENSCH – SICHERHEIT IST MEHR ALS TECHNIK

Gastgeber-Branche bietet viele Einfallstore für Hacker: Jetzt Schutz-Maßnahmen ergreifen!

Die Zahl der Cyberangriffe nimmt weltweit zu. Mehr als die Hälfte der deutschen Unternehmen sind den Gefahren durch digitale Angriffe ausgesetzt. Das geht aus einer Studie des Digitalverbandes Bitkom hervor. Betroffen sind hier natürlich auch die Gastronomie und Hotellerie. So gelangten etwa bei einem Hacker-Übergriff im vergangenen Jahr 500 Millionen Gästedaten der Marriott-Kette in kriminelle Hände. Nun soll der Hotelkonzern eine Strafe von 110 Million Euro bezahlen. Fakt ist, die Gastgeber-Branche wird zunehmend interessantes Opfer für digitale Betrügereien. Einfallstore gibt es reichlich: Fast jeder Betrieb bietet seinen Gästen ein kostenloses W-LAN an. Man arbeitet mit diskreten Kreditkartendaten und offenen Online-Buchungen. Und das Fortschreiten dieser Entwicklung macht es umso wichtiger, diese kritischen Infrastrukturen sowie die sensiblen Unternehmens- und Kundendaten zu schützen. Es gilt, frühzeitig Risiken sowie mögliche Schadensauswirkungen zu identifizieren und Sicherheitsvorkehrungen zu treffen. Doch was nützt diese zurecht essenzielle Vorsorge, wenn der Mensch zu unbedarft handelt? „Etwa 30 Prozent aller Angestellten klicken auf alles, was du ihnen schickst." So plakativ drückte es der IT-Sicherheitsexperte Dmitri Alperovitch in einem Interview mit der Süddeutschen Zeitung aus. Und auch eine Befragung des Bundesamtes für Sicherheit in der Informationstechnik hat ergeben, dass der Mensch der Schlüsselfaktor beim Cyber-Schutz ist. Denn E-Mails oder in die Irre programmierte Webseiten stellen die mit Abstand häufigsten Infektionswege mit Schadsoftware dar. Das Ausspionieren von Daten durch Manipulation von Mitarbeitern ist der neue Trend. „Der Mensch ist wohl das schwächste Glied in der gesamten Sicherheitskette. Die beste Technik reicht nicht aus, wenn der Benutzer durch sogenannte Social-Engineering oder Human-Hacking Angriffe manipuliert wird. Kriminelle finden es offensichtlich einfacher, das Vertrauen von Personen auszunutzen, als sich in technisch sichere IT-Systeme zu hacken", erklärt Dr. Stefan Leinenbach. Er ist der Geschäftsführer der INFOSERVE GmbH, einem saarländischen IT-Unternehmen mit Schwerpunkt IT-Sicherheit und professionellem IT-Betrieb.

Foto: © StockPhotoPro, Adobe Stock

Forscher gehen davon aus, dass rund 80 Prozent der menschlichen Entscheidungen gefühlsbasiert getroffen werden. Der Verstand hat also in vielen Fällen wenig Mitspracherecht. Und genau diesen Umstand nutzt Social-Engineering aus. Das Angriffsziel ist der Benutzer, um ihn zu sicherheitskritischen Handlungen zu verleiten. Doch wie bringt man Mitarbeiter dazu, sich gegen Attacken aus dem Netz zu wappnen? Wenn technische Maßnahmen nicht ausreichen, bedarf es zusätzlicher Werkzeuge. Dies sind in erster Linie Security Awareness-Schulungen. Hier wird das Sicherheitsbewusstsein aller Mitarbeiter geschärft. „Es wäre trügerisch, sich beschützt zu fühlen, nur weil man die neueste IT-Sicherheitstechnologie einsetzt. Genauso wichtig ist, die Belegschaft in regelmäßigen Abständen für die Risiken zu sensibilisieren, sie zu informieren und das richtige Abwehrverhalten im Angriffsfall anzutrainieren", weiß Leinenbach. Die Inhalte solcher Schulungen können vielfältig sein. Doch vor allem müssen sie immer wieder an neue Angriffsmuster angepasst werden. Die Beschäftigten sollten hier unter anderem lernen, Internet-Adressen richtig zu verstehen – und im Zweifelsfall zu misstrauen. Sie sollen mit Mails und deren Anhängen generell skeptisch umgehen. Es gilt, den vermeintlichen Absender kritisch unter die Lupe zu nehmen und vor allem Links in Mails am besten zu ignorieren. Auch sollen stets sichere Kennwörter benutzt und der Computer-Bildschirm beim Verlassen des Büros gesperrt werden.

Dies sind einige grundlegende Beispiele aus einem weitreichenden Katalog von Maßnahmen. Weit mehr kann in sogenannten Social Engineering-Audits erfolgen. Diese zeigen auf, wie es um das IT-Sicherheitsbewusstsein im Unternehmen steht. Das Audit erbringt dabei in der Regel den Beweis, dass eben doch nicht alle Angestellten mit den Gefahren vertraut sind. Die Aufgabe lautet also, mit klassischen Social Engineering-Methoden die Erfolgswahrscheinlichkeit eines bösartigen Ansturms einzuschätzen. Dieser simulierte Angriff kann dabei per Mail, vor Ort oder per Telefon erfolgen. Im Fokus sollten möglichst viele Mitarbeiter stehen, um eine gute Einschätzung des durchschnittlichen Gefahrenpotentials zu erlangen. Die Auswertung erfolgt vollständig anonym und ohne jeglichen Hinweis auf die Kollegen und deren positives oder negatives Verhalten. Es geht hierbei alleine um eine generelle Beurteilung der Sicherheitslage.

Foto: © INFOSERVE

INFOSERVE
eurodata Gruppe

Kontakt
Dr. Stefan Leinenbach, Geschäftsführer
INFOSERVE GmbH
Am Felsbrunnen 15, 66119 Saarbrücken
Telefon: +49 681 8 80 08-0
www.infoserve.de, info@infoserve.de