WIRTSCHAFTSDETEKTEI
S.E.S

SEMINARE FÜR FÜHRUNGSKRÄFTE UND MITARBEITER

Löchriger Käse:
Das Märchen vom geschützten Netzwerk –
Wirklichkeit und Abhilfe

TEIL I: Das Seminar erklärt auf verständliche Weise die wichtigsten und größten Gefahrenquellen in IT-Systemen. Damit richtet es sich vorrangig an Entscheidungsträger und Führungskräfte, die aufgrund Ihrer vielfältigen Aufgaben kaum Gelegenheit haben, sich mit den Details der eigenen IT-Struktur vertraut zu machen. Aber auch in Sachen IT wenig erfahrene Mitarbeiter, die in die Lage versetzt werden sollen, Löcher im System zu erkennen, profitieren deutlich von diesem Seminar. Dieses soll aus unabhängiger Perspektive den Blick schärfen für eine kritische Betrachtung der meist wenig verständlichen Arbeit von Administratoren oder externen IT-Zulieferern. Anhand einer Checkliste ist der Seminarteilnehmer anschließend in der Lage, die wesentlichen Punkte im eigenen Unternehmen abzugleichen. In der als offenes Seminar angelegten Veranstaltung geht der Dozent zudem auf die individuellen Fragen der Teilnehmer ein, gibt weiterführende Hinweise und – soweit im Rahmen des Zeitfensters möglich – auch Lösungsvorschläge für konkrete Problemstellungen. Im Seminar erfahren die Teilnehmer, an welchen Stellen sie besonders hinschauen müssen, was sie stutzig machen sollte und welche Anzeichen es dafür gibt, dass Mitarbeiter manipuliert werden. Außerdem lernen sie die wichtigsten Sicherheitsvorkehrungen beim Betrieb von Computern und Netzwerken kennen und erhalten Einblick in die technischen Möglichkeiten von IT-Spionen. Letztlich gibt das Seminar Aufschluss über das richtige Handeln im Fall des Falles eines Angriffs.

TEIL II: Angeboten wird ein tiefer in die Materie eintauchendes Seminar. Das richtet sich vor allem an im Detail interessierte Führungskräfte, an die Verantwortlichen für IT-Systeme sowie an Administratoren. Inhalt sind unter anderem die Fragen: Werden Mitarbeiter bezogen auf IT-Sicherheit regelmässig geschult? Welche Sicherheitslücken existieren? Wie werden diese eingestuft? Es geht um den Einsatz automatisierter Updates, um die richtigen unternehmensweiten Sicherheitsrichtlinien (Umgang mit Kennwörtern, physikalische Sicherheit etc.), um Konzepte für Hochverfügbarkeit, Load-Balancing und um Server, die über das Internet erreichbar sind und besonderes geschützt werden müssen (Hardening). Weitere Punkte des tiefergehenden Seminares sind Intrusion Detection System bzw. Intrusion Prevention System, die fremdes Eindringen melden und Zero-Day-Exploits abwehren können, sowie Netzwerkmonitoring und Security-Audits. In Kurzform werden die IT-Security-Normen (BSI, ISO 27001, CIS) besprochen, die Teilnehmer erhalten einen Überblick zu Systemen mit normalem Schutzbedarf und hohem Schutzbedarf und lernen den Nutzen von One Time Passwords (OTP) kennen, um beispielsweise Man-in-the-middle-Attacken zu verhindern.

ALLGEMEINE INFO: *Die Seminare sind aufbauend oder unabhängig voneinander buchbar und können für Einzelpersonen aber auch für bis zu acht Teilnehmer in unserem Schulungsräumen in Wuppertal stattfinden. Somit verursachen sie außer der Teilnehmergebühr keine weiteren Kosten. Nach Absprache können Snacks angeboten werden. Kaffee in der Pause ist bei Seminaren in unserem Hause für die Teilnehmer ebenfalls frei. Außerdem besteht auf Wunsch die Möglichkeit, in die Räume des Kunden auszuweichen bzw. das Seminar in anderen Tagungs- und Konferenzstätten stattfinden zu lassen. Infos zum Seminar sind erhältlich über*

eMail an seminar@detektei-ses.de

oder unter freecall 0800/7371000.