Pressemitteilung

Datendiebstahl und Cybercrime

WFG Rhein-Erft informierte Unternehmen

Temperaturen um die 35° C hinderten die rund 50 Gäste der Wirtschaftsförderung Rhein-Erft GmbH nicht, sich am vergangenen Dienstag in der Kommandeursburg in Kerpen-Blatzheim im Rahmen einer Informationsveranstaltung über die Risiken und Herausforderungen in der digitalen Welt zu informieren. Die Geschäftsführerin der WFG Rhein-Erft, Susanne Kayser-Dobiey, freute sich bei der Begrüßung über das große Interesse der kleinen und mittleren Unternehmen: „Offensichtlich haben wir mit „Datendiebstahl und Cybercrime“ ein wichtiges Thema für die Wirtschaft aufgegriffen“.

Datensicherheit ist unabdingbar, wenn Digitalisierung erfolgreich bleiben soll

Peter Vahrenhorst, Spezialist des Cybercrime Kompetenzzentrums beim Landeskriminalamt NRW, informierte als erster Referent des Tages über die aktuell bekannten kriminellen Vorgehensweisen. Dabei ging es nicht nur um die moderne Art einen Geldautomaten zu hacken, sondern auch um die Fragen, wie und warum sich immer mehr Hacker unberechtigten Zugang zu den IT-Systemen von Firmen verschaffen. Vahrenhorst erklärte, „die fortschreitende Digitalisierung bietet in allen Bereichen neue Möglichkeiten für Straftäter“. Wirtschaftsspionage, Sabotage, Datendiebstahl und Erpressung stehen im Vordergrund dieser kriminellen Aktivitäten. Die Schäden durch derartige Angriffe liegen nach aktuellen Schätzungen bundesweit bei 55 Milliarden Euro. Neben finanziellen Einbußen und Ausfällen im Betrieb, sei ein solcher Angriff immer auch mit einem Imageverlust des Unternehmens verbunden. Betroffen sind bereits mehr als 50 % aller Unternehmen. Damit sei Cybercrime eine echte Bedrohung für die Wirtschaft und verlange nach geeigneten Schutzmaßnahmen. Die Bekämpfung sei eine gesamtgesellschaftliche Aufgabe. Alle Akteure – Forschung, Industrie, Lehre, Verbände und nicht zuletzt die Strafverfolgungsbehörden – müssen in gemeinsamen Anstrengungen gegen Cybercrime kooperieren, so das Fazit.

Cybercrime betrifft Behörden, Unternehmen und Privatleute

Mechthild Stöwer, Leiterin der Abteilung Security Management beim Fraunhofer Institut für Sichere Informationstechnologie, appellierte an die Zuhörerinnen und Zuhörer: „Schaffen Sie einen organisatorischen Rahmen für die Informationssicherheit, führen Sie eine Risikoanalyse durch und holen Sie sich Hilfe bei einem IT-Sicherheitsspezialisten“. Der Schaden durch einen Angriff auf IT-Systeme ließe sich begrenzen, wenn diese Empfehlungen vor einem Schadenseintritt beachtet wurden. Technische und organisatorische Sicherheitsmaßnahmen seien ebenso wichtig, wie die regelmäßige Schulung der Mitarbeitenden und die Implementierung eines Informationssicherheits-management Systems. Die Überprüfung, ob eingerichtete Sicherheitsmaßnahmen gut funktionieren, müsse in angemessenen zeitlichen Abständen erfolgen. Unbrauchbare Sicherheitskopien und Backups seien keine Seltenheit, wenn nach einem Schaden eine Wiederherstellung der Systeme und Daten erfolgen soll. Schutz- und Notfallkonzepte mit einer detaillierten Festlegung von Verantwortlichkeiten seien unverzichtbar. Patchmanagement, Rechteverwaltung, Datensicherungskonzept, gesicherte Remotezugänge, Netzsegmentierung, Awareness, Spam Filter, und Notfallkonzept lauten die Schlagworte für dringend erforderliche Sicherheitsmaßnahmen.

Abschließende Botschaft der Expertin an die Unternehmerinnen und Unternehmer: „Halten Sie das Thema selbst kontinuierlich im Blick!

Investitionen in die digitale Sicherheit zahlen sich aus

Eine Demonstration, wie leicht es sein kann, einen anderen PC oder ein IT-Endgerät fremdzusteuern ließ Martin Wundram vom Bundesverband für den Schutz kritischer Infrastrukturen e.V. folgen. Einleitend beschrieb der anerkannte und vereidigte IT-Sachverständige ein Wahrnehmungsproblem bei der Datensicherheit. Bei einem brennenden Auto erkenne jeder sofort die Gefahr und Notwendigkeit zu handeln. Sicherheitslücken in digitalen Medien seien aber auf den ersten Blick nicht erkennbar, die Auswirkungen wären aber teils verheerend. Ein schwimmender Eisberg zeige auch nur einen Bruchteil seiner tatsächlichen Größe. Pokern oder Roulette mit der Datensicherheit zu spielen, könne nicht die Lösung sein. Risikomanagement müsse die Grundmaxime sein. Durch die allgegenwärtigen Smart-Devices sei das Risiko für Angriffe auf It-Systeme erheblich gestiegen. Social-Engineering verstärke die Gefahr in einem weiteren Bereich. Herr Wundram schlug vor, die IT-Unsicherheit als Mangel zu werten, der dringend behoben werden müsse. Umfassende Sicherheitstests einzelner Rechner oder Netzwerke und Sicherheitsaudits seien zwingend. Ebenso das Verlangen, von Anbietern und Kunden ausschließlich sichere Prozesse zu akzeptieren. Hacker hätten genügend Zeit, um an verschiedenen Stellen unbemerkt und in Ruhe eine Sicherheitslücke zu finden. Dabei sei die Sicherheitskette immer nur so stark, wie ihr schwächstes Glied.

Der Faktor Mensch ist häufig die Schwachstelle

Die beiden Experten Felix Eifert und Daniel Kant des Kompetenzzentrums IT-Wirtschaft Mittelstand 4.0 von der technischen Hochschule Brandenburg gaben abschließend Empfehlungen, wie man sich vor unberechtigtem Zugriff schützt. Technische Sicherheitsmaßnahmen gegen das Ausnutzen von Schwachstellen zum Beispiel durch Phishing, Ransomware und Trojaner sind vor allem die 2-Faktor-Authentifizierung, die Deaktivierung von USB-Schnittstellen, Sand Boxing und Container-Lösungen. Awareness-Bildung und Schulung von Mitarbeitenden gehöre ebenfalls zum Basis-Schutz. Als weiteres Risikoszenario wurden diverse Webserver-Angriffe vorgestellt und mit welchen Vorkehrungen die Sicherheit erhöht werden kann. Beispielhaft wurden hier die Einrichtung von Timeouts an den Geräten, die Nutzung komplexer Passwörter und Authentifizierungssysteme, Firewalls und die Deaktivierung von unnötigen Diensten und Ports erläutert. Zum Abschluss erläuterte Daniel Kant, dass durch die Nutzung mobiler Endgeräte -insbesondere durch infizierte private Tablets oder Handys – wesentliche Schäden für Unternehmen entstehen. Der Einsatz von Verschlüsselungstechniken und Antiviren-Apps für Smartphones, die Nutzung von VPN Verbindungen und die Möglichkeit des Löschens per Fernzugriff seien hilfreich bei der Schadensbegrenzung.

Informationsstände der Wirtschaftsförderung Rhein-Erft GmbH, des Bundesverbands für den Schutz kritischer Infrastrukturen und des Bundesamtes für Sicherheit in der Informationstechnik rundeten das Angebot der Fachtagung ab.

Hajo Thiesen, Projektleiter Digitalisierung bei der WFG Rhein-Erft, freute sich über die hervorragenden Beiträge der Referenten und den positiven Verlauf der Veranstaltung. Nach fast zweieinhalbstündiger Informationskonzentration bedankte sich Susanne Kayser-Dobiey bei allen Akteuren, die bei allen Gästen das Thema Datensicherheit noch einmal deutlich in den Vordergrund geholt haben. Beginnend mit den Darstellungen zur aktuellen Bedrohungslage durch kriminelle Energie, die Erläuterung der notwendigen organisatorischen Maßnahmen zur IT-Sicherheit, die Demonstration eines Live Hackings und die Empfehlungen zum Schutz vor unberechtigtem Zugriff auf IT-Systeme und Daten konnten die Gäste ein rundes Paket an Informationen zu Datensicherheit und Cybercrime mitnehmen. Zum Ausklang der Informationsveranstaltung gab es für die Gäste ergänzend die Möglichkeit, Fragen an die Referenten zu stellen und die Zeit des Networkings für den Aufbau neuer Kontakte zu nutzen.