POLIZEI Hamburg

IT-Sicherheit

In den vergangenen Wochen wurden viele Menschen von IT-Sicherheitsvorfällen aufgeschreckt. Eines vorweg: Das polizeiliche IT-Netz und seine Daten waren nicht gefährdet. Allerdings werden die Angriffsversuche immer ausgefeilter. Deshalb einige vorsorgliche Hinweise für den Dienstbetrieb.

Kategorien
Sicherheit; IT

IT-Sicherheit KOMPAKT

In den vergangenen Wochen wurden viele Menschen von IT-Sicherheitsvorfällen aufgeschreckt. Eines vorweg: Das polizeiliche IT-Netz und seine Daten waren nicht gefährdet.
Allerdings werden die Angriffsversuche immer ausgefeilter. Deshalb einige vorsorgliche Hinweise für den Dienstbetrieb.
Im E-Mail-Verkehr sollte darauf geachtet werden, nur solche E-Mails zu öffnen, die man üblicherweise erhält und für die ein tatsächlicher dienstlicher Bezug besteht. Ansonsten sollten Sie derartige E-Mails (bspw. die Rechnung eines Telefonanbieters bei dem überhaupt kein Telefonvertrag besteht) schlichtweg löschen. Keinesfalls sollten Sie angehängte Dokumente öffnen oder gar die erbetene Antwort versenden.
Damit polizeiliche Namen oder E-Mail-Adressen nicht im Internet „abgefischt" werden, dürfen sie nicht in Internetportalen für Einkäufe oder „soziale" Netzwerke verwendet werden, wenn dies nicht im Vorwege dienstlich autorisiert ist.
Keinesfalls dürfen Dienste im Internet wie WhatsApp für die polizeiliche Kommunikation oder als Ersatz für vermeintlich notwendige, aber nicht vorhandene „Kommunikationskanäle" genutzt werden. Ein aktuelles Beispiel aus der schwedischen Polizei finden Sie auf spiegelonline. Dadurch wurde nicht nur die polizeiliche Arbeit negativ beeinflusst, sondern es flossen auch polizeiliche Informationen und Daten an Unberechtigte ab.
Ebenso wenig darf die dienstliche Terminplanung auf privaten Geräten oder über E-Mail-Konten im Internet erfolgen. Der Grund ist einfach: Mit der Terminplanung und etwaigen Besprechungsanfragen werden nicht nur die Namen der polizeilichen Mitarbeiter veröffentlicht, sondern es werden auch Dokumente zu dem jeweiligen Thema übermittelt. Auf diesem Wege würden dann polizeiliche Inhalte abfließen. Damit würden die Anstrengungen der Polizei, das polizeiliche IT-Netz und die darin enthaltenen Daten nach außen abzusichern, unterlaufen werden.
Das Internet in der beschriebenen Weise für dienstliche Aufgaben zu nutzen, würde gegen bestehende dienstliche Anordnungen verstoßen und kann zumindest disziplinare Maßnahmen nach sich ziehen.
Ergänzend wird nochmals darauf aufmerksam gemacht, dass private Geräte weder an dienstliche PC noch an die polizeiliche Netzinfrastruktur angeschlossen werden dürfen.
Sofern Ihnen Sicherheitslücken, bspw. allgemein zugängliche persönliche Verzeichnisse auf einem Server, auffallen, informieren Sie bitte den jeweils für die Benutzerverwaltung Verantwortlichen („BV-User").
In allen anderen Fragen steht Ihnen das IT-Sicherheitsmanagement per E-Mail unter [redacted] oder telefonisch unter [redacted] zur Verfügung.
Im FHH-Netz besteht ein Training, das die Grundlagen eines sicheren und verantwortungsbewussten Umgangs mit PC und Daten sowohl für dienstliche Aufgaben als auch im privaten Umfeld vermittelt. Auch der Polizei steht das „Behörden-IT-Sicherheitstraining - BITS" jetzt zur Verfügung. Am Ende der jeweiligen Lektion gibt es nach der Zusammenfassung dann auch einen kleinen Wissenstest. Probieren Sie es einfach mal aus!

Weiterführende Informationen:

Links

Behörden-IT-Sicherheitstraining - BITS

Mitarbeiterinformation zur IT-Sicherheit