Sollte der Newsletter nicht richtig angezeigt werden, klicken Sie bitte hier.

Security SFS Finder Schweiz

Sehr geehrte Damen und Herren,

In den letzten Jahren sind Industriespionage-Fälle und Angriffe durch Malware und Viren exponentiell angestiegen. Hacking ist nach wie vor ein ernstes und organisiertes, globales Phänomen, das von Staaten, politischen Parteien und konkurrierenden Marktteilnehmern gefördert wird. Stichworte: Ragemaster oder Nightwatch.

Zu glauben, dass Ihr Unternehmen nicht Ziel von Cyber-Angreifern wird, weil es klein oder lokal aufgestellt ist und kein geistiges Eigentum hat, ist ein verständlicher, aber fehlgeleiteter Ansatz. Denn fortgeschrittene Cyber-Bedrohungen sind eine echte und unmittelbar bevorstehende Gefahr. Am besten schützen Sie Ihr Unternehmen, indem Sie sich über die vorhandene Bedrohungslandschaft informieren und mit der Einrichtung einer soliden Cyber-Sicherheitsstrategie beginnen.

Cyber in Ihrem Unternehmen? Versichern Sie sich!

Herzlich.
Roger Eric Gisi

Cyber-, IT- und Cloud-Security auf der App **Cloud Schweiz**

EDÖB rät von Auslagerung ins Ausland ab

Auch zur heiklen Frage der Auslagerung von Behördendaten ins Ausland nimmt der Eidgenössische Datenschutzbeauftragte, Hanspeter Thür, in seinem kürzlich veröffentlichten Tätigkeitsbericht 2014/2015 Stellung. Aufgrund der akuten Gefahr von Zugriffen durch ausländische Behörden rät er Bundesorganen davon ab, Datenbearbeitungen an Cloud-Anbieter auszulagern, die ihren Sitz in den USA oder in anderen Staaten ohne gleichwertiges Datenschutzniveau haben.

Nationale Regelungen greifen zu kurz

In der EU arbeitet man daran, einheitliche Datenschutzgrundlage zu schaffen. Da man Daten im Zeitalter von Cloud-Computing und Big Data in immer stärkerem Ausmass grenzüberschreitend nutzt, ist laut Expertin Ursula Widmer jede Vereinheitlichung des dabei massgeblichen rechtlichen Rahmens grundsätzlich zu begrüssen. Denn: «Nationale rechtliche Regelungen greifen hier einfach zu kurz und lassen sich häufig gar nicht mehr wirksam durchsetzen.»

Privatsphäre in Gefahr

Im Bereich der staatlichen Überwachung richtete sich der Fokus des EDÖB auch dieses Jahr auf das neue Nachrichtendienstgesetz (NDG) und das Gesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). Die Erweiterung der Überwachungs- und Informationsbeschaffungs-Massnahmen um Staatstrojaner, IMSI-Catcher und andere birgt beträchtliche Risiken für die Privatsphäre. Bei beiden Gesetzen setzt er sich deshalb dafür ein, dass der Einsatz dieser Mittel klar definiert wird und nicht ohne richterliche Anordnung erfolgt.

Unsere Abhängigkeit nimmt zu

Abgesehen von Nischenprodukten ist die Schweiz zu einem Importeur und Konsument von ICT-basierten Leistungen geworden. Wir sind angewiesen auf die Verfügbarkeit, Funktionsfähigkeit und Zuverlässigkeit von globalen Akteuren. Damit hat die Schweiz die digitale Autonomie und Kontrolle über Daten, Wertschöpfungsketten und Netzwerke weitgehend verloren. Wir sind faktisch (und zunehmend auch rechtlich) digital nicht mehr souverän – weder als Individuen noch als Gesellschaft oder als Staat.

Bund will Kommunikationsnetz für Krisenlagen

Eine anhaltende Strom-Unterversorgung würde eine «komplexe nationale Notlage» bedeuten. Darum hat der Bundesrat das VBS beauftragt, ein sicheres Datenverbundnetz zu schaffen. Das Netz soll in Krisenlagen die Verbindung innerhalb des Sicherheitsverbundes Schweiz ermöglichen – also zwischen Führungsanlagen der Landesregierung, allen Departementen, Kantonen und Betreibern kritischer Infrastrukturen wie Flughäfen und Kernkraftwerken.

Für Strommangel schlecht gerüstet

Sollte es zu einem mehrwöchigen Strommangel kommen, wäre die Schweiz schlecht gerüstet. Zu diesem Schluss kommt ein Bericht zur Sicherheitsverbundsübung (SUV) 2014. Schwerwiegende Mängel ortet der Bericht insbesondere bei der vernetzten Führung und Koordination. Ins Gewicht falle etwa, dass Bund und Kantone nicht über ein integrales Lagebild verfügen. Grundsätzlich genügen würden hingegen Technik und Infrastruktur der Führungsorgane, um die Krise zu bewältigen.

RISIKO-MANAGEMENT

Do you Know the Key to Security?

As we edge closer into this digital world, the speed in which technology is evolving to change our physical and intellectual world is fast – everything becomes digital. Have you asked yourself how you can protect yourself around this digital landscape and safeguard what matters most? Expert Thomas Koch from PwC Switzerland has knowledge about what will help you to engage your employees when it comes to security awareness.

5 Growing Pains for Chief Data Science Officers

Avoiding perpetuating «ivory tower» perceptions, building relationships with the c-suite, finding the funding, navigating the vendor landscape and changing the decision-making mindset of executives – according to PwC, those are the growing pains Chief Data Science Officers (CDSO) are faced with. If businesses can't find a way to properly address some of these issues, the role of the CDSO could be at risk.

SICHERHEITSEXPERTEN

Marco Rohrer - Geschäftsführer IPG AG

Marco Rohrer, Dipl. Betriebsökonom FH mit Vertiefungsstudium in Entrepreneurship sowie Vertiefungskursen in Organisation & Marketing, leitet heute als Geschäftsführer die IPG AG in Winterthur.

INFORMATIONS- UND IT-SICHERHEIT

Chart your Course Toward Cyber Security

Cyber security is a constant, and, by all accounts, a growing challenge. A recent report shows that organizational size and software quality play significant roles in the strategies that defenders may adopt and that those who secure networks will have to pay increasing attention to the role that smart devices might otherwise play in allowing hackers in. Organizations could benefit from better understanding their risk posture, better defining the role of government, and exploring information sharing responsibilities.

Angriff und Abwehr: Ein ungleicher Kampf

In den letzten Jahren mussten sich Cyber-Security-Verantwortliche mit einer neuen Art von Gefahren auseinandersetzen: Gezielte Angriffe und APTs. Sie sind eine der ausgereiftesten Formen von Cyber-Angriffen, da gut ausgerüstete und fähige Gegner sie mit präzisen Absichten schaffen. So entsteht laut Marc Stöcklin von IBM ein ungleicher Kampf. Denn ein Angreifer muss nur einmal richtig raten, der Verteidiger muss aber immer richtig liegen. Existierende Sicherheitsmechanismen und -technologien können solche Gefahren im Normalfall nicht aufspüren und verhindern.

Schwachstellen unter der Lupe

Mit der Schweiz assoziiert man Qualität und Sicherheit. Doch die IT-Systeme im Schweizer Internet weisen teils gravierende Sicherheitsmängel auf. Das zeigt der aktuelle Swiss Vulnerability Report der First Security Technology AG (FST). Für den Report stellte FST Anfragen an die Dienste aller Schweizer IP-Adressen, die ans Internet angebunden sind. Diese aktiven Dienste geben automatisch Auskunft über die verwendeten Betriebssysteme, Applikationen und deren Version. Die Auswertung dieser Informationen bringen viele interessante Erkenntnisse ans Tageslicht.

How Good is your Security Operation Center?

Many organizations operate a dedicated department specifically for combatting cyber security threats, typically called Security Operation Centers (SOC). Today, managing a SOC and meeting the increasing expectations of key stakeholders is a big challenge. Useful strategies that can help to address this are: know the enemy, the business, the assets, the data and your staff. Transforming the SOC to meet today's challenges requires an intelligent approach to how companies manage cyber security and its own critical information assets.

Wie die Integritätskontrolle bei Big Data möglich wird

Die Integrität der Daten als Schutzziel stellt bei Big Data besonders hohe Anforderungen, ist aber für den Datenschutz und den Wert der Analysen unerlässlich. Zur Integritätsüberwachung sind generelle Methoden wie Protokollierung und Identitäts- und Zugriffsmanagement möglich. Die enormen Datenmengen und die komplexen Berechtigungsstrukturen machen aber schnelle, leistungsstarke Lösungen unerlässlich.

45% der verschlüsselten Verbindungen sind auf Poodle anfällig

Der aktuelle Swiss Vulnerability Report analysiert Schwachstellen in der SSL- und TLS- Verschlüsselung vertieft. Heartbleed und Poodle sind in aller Munde. Prüfungen auf die Schwachstelle Poodle im Februar und Mai machen die Notwendigkeit der Behebung deutlich: Ende Mai 2015 waren laut Report noch 45% der verschlüsselten Verbindungen auf Poodle anfällig. Vermeintlich sichere Verbindungen sind abhörbar.

Gartner; Exostructure's Importance to Rise

According to Gartner, exostructure is one of the top 10 strategic technologies impacting education this year. When done right, it enables institutions to leverage services from the cloud, rather than having to bring them inside the campus walls. Enabled by standards, it can allow the institution to adapt faster. With the increasing interdependencies in the education ecosystem, Gartner sees it rising in importance for at least the next decade. The future belongs to exostructure rather than to infrastructure.

Cloud-Anbieter in der Schweiz empfohlen

Der Trend, Daten in einer Cloud statt auf dem eigenen Rechner aufzubewahren, macht auch vor Ärzten nicht halt. Wegen ihres im Strafrecht verankerten Berufsgeheimnisses ist das jedoch problematisch. Der EDÖB weist darauf hin, dass Ärzte auch bei einer Auslagerung der Patientendaten für deren Geheimhaltung verantwortlich bleiben. Er legt ihnen nahe, Cloud-Anbieter mit Sitz in der Schweiz zu wählen und sich von diesem vertraglich zusichern zu lassen, dass die gespeicherten Patientendaten nicht ins Ausland übermittelt werden.

SECURITY-KALENDER

«Symposium on Privacy and Security», ETH Zürich

Big Data und Big Data Analytics bleiben die aktuellen Herausforderungen und werden unsere Gesellschaft in Zukunftin hohem Ausmass prägen. Darum sind sie zwei der Schlüsselthemen des «Symposium on Privacy and Security» am 27. August. Marc Elsberg, Autor von «Zero – Sie wissen, was du tust», zeigt in seinem Referat «Carte Blanche»: Wert und Macht» auf, wie unkontrollierte Datensammlung und -verwertung alle Werte kommerzialisieren und die Fundamente unserer demokratischen Gesellschaft aushöhlen.

CAS Cloud-Computing: Schon angemeldet?

Die FHNW-Weiterbildung «CAS Cloud-Computing» vermittelt Ihnen fundiertes Verständnis von Cloud-Computing. Das 15-tägige CAS-Programm bereitet Sie von 4. September bis 28. November 2015 auf Cloud-Herausforderungen wie Cloud-Strategie, Interoperabilität, Integration, Compliance und Sicherheit vor. Dank dem neuen Wissen können Sie Licht in die oftmals so nebulöse Wolke bringen.

Weitere Security-Termine

18.08.2015	IT-Beschaffungskonferenz 2015; Bern
25.08.2015	Frühstücks-Workshop IAM; Zürich City
27.08.2015	20. Symposium on Privacy and Security; Zürich

Zum Security-Kalender

Expertenthemen zu Cloud, Cloud-Security und Applications CRM/XRM/CEM finden Sie hier.