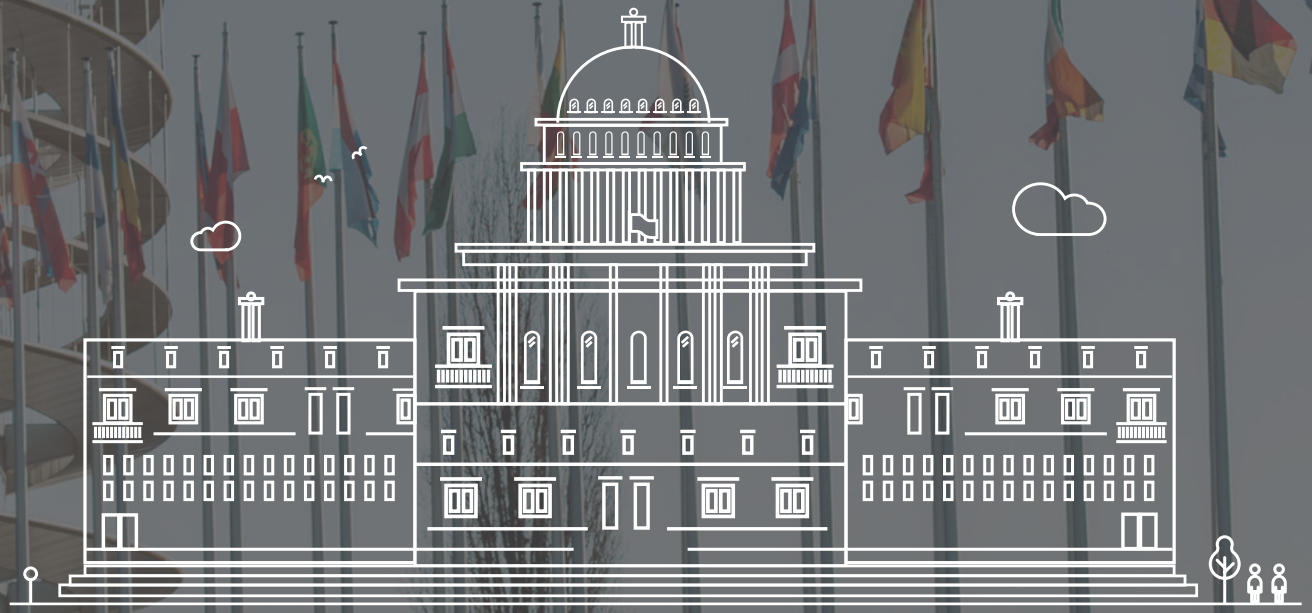
Ausgabe Schweiz

Datenschutz in der öffentlichen Verwaltung



pandasecurity.com

panda

Technologische Technokratie

Der öffentliche Sektor erlebt derzeit eine noch nie dagewesene Transformation durch die Verwendung neuer Technologien in allen Bereichen des öffentlichen Diensts.

Die Einführung neuer Technologien ist ein wichtiger Faktor in der Verbesserung der Prozesse und des Wachstums der Wirtschaft. In der Tat hat das Niveau der staatlichen Eingriffe in die nationalen Volkswirtschaften in den letzten Jahren einen neuen Höchststand erreicht. Laut EUROSTAT erreichten die Ausgaben des öffentlichen Sektors in der EU 48,2 Prozent, dies entspricht beinahe dem Beitrag der produktiven Wirtschaft und unterstreicht das Ausmass, in dem unser Leben von der öffentlichen Verwaltung beeinflusst wird.

Die Nutzung von Informations- und Kommunikationstechnologien im Allgemeinen und im Besonderen der Online-Behördendienst, sind Schlüsselfaktoren in der Art und Weise wie sich der öffentliche Sektor verändert, ein schneller Zugang zu öffentlichen Diensten sowohl für Privatpersonen und Unternehmen wird immer wichtiger.

Allerdings hat **die Einführung moderner Technologien auch Nachteile, öffentliche Stellen sind nun auch den neuen Arten von Bedrohungen ausgesetzt.** Es ist nun nicht mehr ausreichend typische IT-Probleme zu beachten, wie die Prävention oder die Meldung von Störungen. Die Bedrohung ist real und allgegenwärtig durch Cyber-Attacken.

Der beste Beweis dafür ist, der im Mai dieses Jahres erfolgte Angriff auf den Schweizer Rüstungskonzern Ruag. Der eingesetzte Malwaretyp war bereits seit 2008 bekannt dafür, dass er für Computer-Angriffe auf Regierungsstellen angewendet wird. Mit Beginn des Jahres 2014 häuften sich die Turla-Angriffe. Opfer der Angriffe waren vor allem öffentliche Einrichtungen in Europa (auch der Schweiz). Im Fall Ruag "lebte" die Malware seit beinahe einem Jahr im System, bevor sie entdeckt wurde. Laut technischen Bericht der Melde- und Analysestelle Informationssicherung (MELANI) zeigten die Angreifer viel Geduld bei der Infiltration und griffen nur Opfer an, die von strategischen Interesse waren, um an Geräte mit höheren Privilegien zu gelangen.

Die technologische Revolution im öffentlichen Sektor, die Digitalisierung und Speicherung von Informationen und der Boom bei Online-Diensten, zur Vereinfachung der Verwaltung, führten zu exponentiellem Wachstum in der Generierung, Speicherung und Verarbeitung vertraulicher Daten; Daten, die mit grösster Sorgfalt behandelt werden. Daher muss sich der öffentliche Dienst neuen Herausforderungen in der Risikovermeidung, Sicherheit und den gesetzlichen Vorschriften stellen.

Viele öffentliche Einrichtungen haben neue Technologien implementiert, ohne den neuen Anforderungen Beachtung zu schenken. Es bedarf nun grosser Anstrengungen sich den neuen gesetzlichen Rahmenbedingungen anzupassen.

Die Aufgabe der Cyber-Sicherheit

Cyber-Bedrohungen sind ein konstantes und erhebliches Sicherheitsrisiko für die öffentliche Verwaltung. So sehr, dass sie zu einer mächtigen Waffe bei Angriffen auf Bürger und Behörden der Länder geworden sind. Derartige Bedrohungen können die Qualität der Dienstleistungen ernsthaft beeinträchtigen und vertrauliche Daten der Gefahr der Offenlegung aussetzen, von privaten Daten bis zu Staatsgeheimnissen.

Die heutige digitale Gesellschaft ist der grösste Nutzniesser dieser technologischen Fortschritte, aber sie muss diese Ressourcen auch verantwortungsvoll und effektiv nutzen. Cyber-Sicherheit ist ein Schlüsselfaktor in der Verbesserung der Benutzererfahrung, Einhaltung gesetzlicher Vorschriften und dem notwendigen Schutz öffentlicher Einrichtungen.

Ursprünglich war IT-Sicherheit ein reaktiver Schutz, aber hat sich nun zu einem proaktiven Schutzmechanismus entwickelt, mit der Identifizierung und Bekämpfung von Cyber-Bedrohungen und ist mittlerweile zu einem globalen Sicherheitsmodell geworden.

Bei jeder Form von Sicherheit liegt die erste Verantwortung bei der Regierung. In der Vergangenheit wurden diese Bereiche in den Abteilungen für Verteidigung verwaltet, da die wichtigsten Bedrohungen von Ländern mit militärischer Natur zu erwarten waren. Heutzutage, in einer hyper-vernetzten Welt gibt es neue Akteure und Risiken, sodass Regierungen nun gezwungen sind ihre bisherige Sicherheits- und Verteidigungspolitik zu hinterfragen und neu zu überdenken.

In den letzten Jahren zeigte sich diese Trendwende auch in der Gesetzgebung einiger Länder und damit verstärkt auch der Einfluss auf die Nutzung und Verwaltung von Kommunikationstechniken im öffentlichen Sektor, sowie auf die Interaktion mit Bürgern und Unternehmen und auch zwischen nationalen, regionalen und lokalen Regierungsbehörden.

Diese Gesetze waren eine echte regulative, organisatorische, technologische und operative Änderung für den öffentlichen Sektor, mit besonderer Auswirkung auf die Nutzung des Internets als Kanal der Interaktion zwischen Bürgern und Behörden, die wahre Öffnung der Regierungen in die Online-Welt.

Die neuen Rechtsvorschriften verlangten nach Grundsätzen und Anforderungen an die Sicherheitspolitik zur Regelung der Nutzung elektronischer Medien für einen angemessenen Datenschutz. So entstanden nationale Sicherheitsstrukturen zur Wahrung der Datenvertraulichkeit in der Nutzung elektronischer Medien zwischen Bürgern und Behörden.

Cyber-Angriffe:

Datendiebstahl

Israels Ministerium für soziale Sicherheit und Wohlbefinden

In den letzten zehn Jahren haben wir verschiedene Arten von Angriffen auf öffentliche Verwaltungen erlebt. Ein Beispiel ist Israels Ministerium für soziale Sicherheit und Wohlbefinden und deren Computer-Wartungsfirma Shalom Bilik. Bilik hatte Zugriff auf die Datenbank und stahl die Daten von neun Millionen Israelischen Bürgern. Die Information wurde verkauft und der Diebstahl blieb unbemerkt bis 2012, als Bilik und fünf weitere Personen, die in diesen Diebstahl verwickelt waren, offiziell angeklagt wurden.

Daten von 9 Millionen Israelischen Bürgern gestohlen.

US Departement of Veteran Affairs

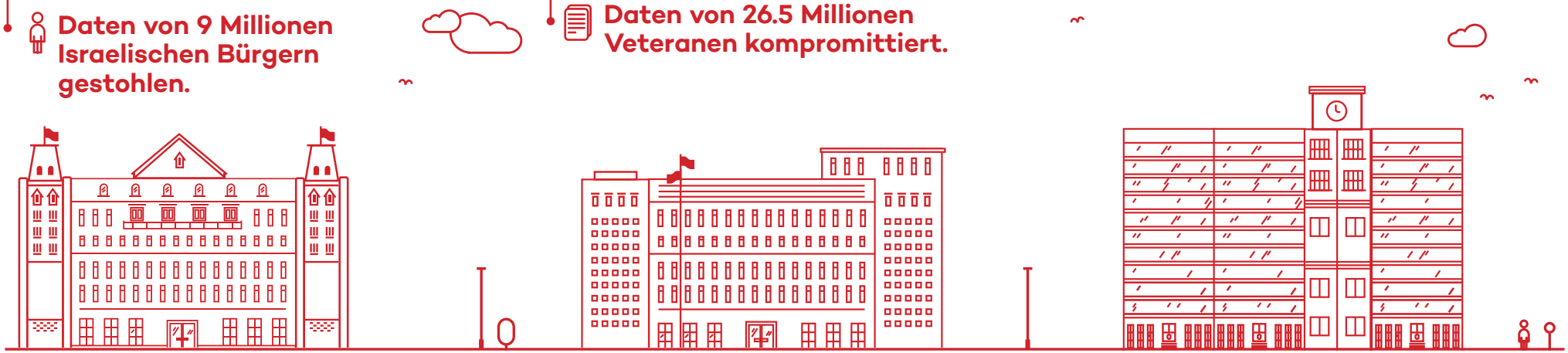
Nicht einmal unsere eigenen Häuser sind sicher und noch weniger, wenn es um die Verwahrung von staatlichen Dokumenten geht. Man kann eine Lehre aus dem Fall des Mitarbeiters des US Departement of Veteran Affairs ziehen, dessen Haus im Mai 2006 ausgeraubt wurde und vertrauliche Daten von 26,5 Millionen Veteranen, einschliesslich Geburtsdatum und Sozialversicherungsnummer entwendet wurden. Der Mitarbeiter hatte an einer statistischen Erhebung gearbeitet und die Daten unerlaubt nach Hause mitgenommen.

Daten von 26.5 Millionen Veteranen kompromittiert.

UK HM Revenue and Customs (Steuerbehörde)

Ein weiterer Fall von Datenmissbrauch fand im Jahr 2007 statt, als zwei Festplatten des HM Revenue and Customs (britische Steuerbehörde)mit den persönlichen Daten von Familien mit Kindern unter 16 Jahren in Grossbritannien verloren gingen. Eine Kurier-Firma war mit der Lieferung beauftragt, die Festplatten erreichten jedoch nie ihr Ziel. Die gestohlenen Daten enthielten Namen, Adressen, Geburtsdaten und Bankverbindungen.

Datenverlust aller UK Familien und mit Kindern.



Das Weisse Haus

Im Jahr 2015 bestätigte Ben Rhodes, stellvertretender nationaler Sicherheitsberaterin den Vereinigten Staaten, dass das Weisse Haus Opfer eines IT-Angriffs gewesen war. In einem Interview mit CNN, bestätigte Rhodes, dass die Angreifer durch nicht autorisierten Zugriff geheime Daten gestohlen hatten. Das System wurde nicht gehackt.

US Amt für Personalmanagement

Im Juni des gleichen Jahres wird berichtet, dass das Amt für Personalmanagement, die Personalagentur der US-Bundesregierung kompromittiert wurde und Daten von mindestens 4 Millionen im öffentlichen Dienst Beschäftigten, gestohlen wurden. Der Angriff erfolgte zwei Monate vor dem Angriff auf das Weisse Haus. Es bestand jedoch kein Zusammenhang zwischen den beiden Attacken.

Zugriff auf geheime Daten.

Zugriff auf vertrauliche Daten von 4 Millionen öffentlich Bedienstete.

Insider

Wie in vielen anderen Bereichen wurden die meisten Datendiebstähle bis 2011 von internen Mitarbeitern mit Zugang zu Informationen durchgeführt. Angriffe von Mitarbeitern mit privilegiertem Zugang sind eine der grössten Bedrohungen für die IT-Sicherheit von Ländern und Unternehmen gleichermassen. Egal ob es sich um einen ausländischen Spion, einen von Terroristen entführten Mitarbeiter oder einen unzufriedenen Mitarbeiter, der aus Trotz stiehlt, handelt-es sind immer Branchenkenner.

Bradley Manning

Einer der berüchtigtsten Datendiebstähle unserer Zeit fand im Jahr 2010 statt, als Bradley Manning, ein US Soldat, 700'000 vertrauliche Dokumente kopierte und mit WikiLeaks veröffentlichte.

Insgesamt waren es fast eine **halbe Million Datensätze aus dem Irak und Afghanistan Konflikt und mehr als 250'000 geheime US-Diplomaten Nachrichten.** Manning wurde wegen Verstosses gegen die Bundesgesetzte zur Veröffentlichung von Verschlusssachen, wegen Lieferung geheimer Berichte an den Feind und Verletzung der IT-Sicherheits- und Hacking-Sicherheitsprogramme, sowie Spionage angeklagt.

Edward Snowden

Es gab einen weitere Fall in den letzten Jahren, der sowohl die CIA und auch die NSA(National Security Agency) in einen Alarmzustand versetzte. Eduard Snowden, ein ehemaliger Mitarbeiter des NSA veröffentlichte 2013 streng geheime Dokumente der verschiedensten NSA Programme, inklusive Massenüberwachungsprogramme PRISM und Xkeyscore. Diese Informationen wurden im Guardian und in der Washington Post veröffentlicht.

Das United States Department of Justice bezeichnete Snowdens Teilnahme am Überwachungsprogramm PRISM als kriminellen Akt, sein Schicksal ist reine Spekulation.

Er kopierte 700'000 vertrauliche Dokumente.

Snowden veröffentlichte streng geheime Dokumente verschiedener NSA Programme.

Angriffe auf Netzwerke und Systeme

Mit fortschreitender Technologie und der zunehmenden Verbundenheit von Systemen, haben Cyber-Kriminelle nun mehr Mittel und Werkzeuge um Angriffe durchzuführen, wie man in den letzten Jahren auch beobachten konnte.

Im Jahr 2012 erlangte ein Cyber-Angreifer Zugriff auf Daten von 3,8 Millionen Steuerzahlern mit einer einfachen E-Mail an die Mitarbeiter des South Carolina Finanzministeriums. Die gestohlenen Informationen enthielten Sozialversicherungsnummern und Bankdaten.

Ein ähnlicher Angriff fand in Monterey County statt, die Angreifer kompromittierten das Netzwerk des Sozialamts und persönliche Daten von 145'000 Einwohnern wurden gestohlen, Sozialversicherungsnummern mit Namen und Adressdaten.

Eine E-Mail verschaffte einem Angreifer Zutritt zum internen Netzwerk und Daten von 3,8 Millionen Steuerzahlern.

Sozialversicherungsnummer und Bankdaten wurden gestohlen.

Politisch motivierte Angriffe

In 2015 gab e seine Vielzahl politisch-motivierter Attacken auf öffentliche Einrichtungen (einschliesslich Hacking sozialer Netzwerken zur Verbreitung von Propaganda) sowie Spionage auf Politiker und hochrangige Beamte.

Cyber-Terrorismus und Cyber-Spionage

Organisierte kriminelle Netzwerke (Cyber-Banden) haben damit begonnen Ihre Aktivitäten verstärkt in den Cyber-Space zu verlegen, sie profitieren so von der Anonymität des Internets um an sensible Informationen zu gelangen und diese dann in betrügerischer Absicht für finanziellen Gewinn einsetzen.

Im Januar 2015, gerade als Barack Obama eine Reihe von Gesetzesinitiativen ankündigte, konnte eine Gruppe von Angreifer mit Verbindung zu ISIS die Kontrolle über die wichtigsten sozialen Netzwerke des Pentagon erlangen. Für diesen Akt mussten sie Zugriff auf E-Mail Konten, Passwörter, Benutzernamen etc haben, Daten und Anmeldeinformationen die normalerweise das erforderliche Sicherheitsniveau haben um Angriffe und Missbräuche zu vermeiden.

Terroristen und extremistische Gruppen verwenden nun den Cyber-Space um Ihre Angriffe zu planen und Anhänger zu rekrutieren.

Diese Taktik wurde von einer Gruppe namens „syrische elektronische Armee“ verwendet, die auf der Webseite der US-Marine, Propaganda für Assads syrisches Regime veröffentlichte.

Die US Regierung wurde abermals Ziel eines Angriffs, als James Comey, Chef des FBI in einem Sicherheitsforum verkündete, dass sie ein wachsendes Interesse der Terroristen für Cyber-Angriffe gegen die USA erkannt hätten. Ohne auf Details einzugehen, erklärte er, dass diese Kriminellen offensichtlich noch in der Planungsphase sind. Dennoch ist dies möglicherweise ein Problem mit schwerwiegenden Folgen.

Mit der Sabotage von Industrieanlagen, Attentate auf Wissenschaftler und der Verwendung des **Stuxnet Computer-Virus begann die geheime Phase des Krieges gegen den Iran.** Während der letzten zehn Jahre sind Spionagedienste der USA und des israelischen Geheimdienstes zu dem Schluss gekommen, dass der Iran eine Urananreicherungsanlage entwickelt hatte. Dies wurde öffentlich nach einer Ankündigung von Barack Obama im

September 2009.

Hacktivismus

Diese Bewegung entstand in 2011, als Hacktivismus zur ernsthaften Bedrohung für Regierungen und Behörden wurde. Die Grundprinzipien sind Anonymität und die freie Verbreitung von Informationen über den Cyberspace, im Wesentlichen über das Internet. Hacktivisten haben eine dezentrale Struktur und nutzen ein verdecktes Netzwerk, um ihre Pläne und Aktionen zu kommunizieren.

Das deutsche Parlament wurde Opfer eines Angriffs, bei dem verschiedenste Computer kompromittiert und Daten gestohlen wurden. Man vermutet, dass der Angriff von Russland aus gesteuert wurde, es fehlen jedoch die Beweise.

Am 25. Juli 2015 gelang einigen russischen Hackern der Zugriff auf das gesicherte E-Mail System des Pentagon. Nach offiziellen Angaben handelte es sich um eine hochentwickelte Attacke, die wahrscheinlich von einer Regierung gestartet wurde.

Ebenso in diesem Jahr, gelang es drei Gruppen lateinamerikanischer Angreifer die Mail-Server der bolivianischen Armee zu gefährden, E-Mails herunterzuladen und davon einige zu veröffentlichen. Die Angreifer hatten leichtes Spiel und verschafften sich Zugriff durch eine alte Sicherheitslücke im Zimbra VMware Dienst, den der Techniker der Armee vergessen hatte zu aktualisieren.

Öffentliche Verwaltungen auf der ganzen Welt, insbesondere Verteidigung und nationale Sicherheitsdienste sind sich der Risiken, denen sie ausgesetzt sind, bewusst. In 2016 stellte das **US Verteidigungsministerium ein Pilotprojekt namens “Hack das Pentagon” vor, es wurden Belohnungen für Hacker angeboten, die Sicherheitslücken in der Webseite des Pentagon, den Anwendungen sowie Netzwerken aufdecken.**

Russische Hacker kompromittierten das frei zugängliche E-Mail System des Pentagon.

Lateinamerikanische Hacker kompromittieren die E-Mail Server der Bolivianischen Armee.

Trotz der enormen Investitionen in die IT-Sicherheit durch die US-Regierung, wurde erst wieder vor kurzem eine gezielte Attacke auf das US Democratic National Committe, die über ein Jahr dauerte, ans Licht gebracht. Auf der Grundlage von gesammelten Beweismaterial liegt der Verdacht nahe, dass es sich hierbei um Angreifer aus dem russischen Nachrichtendienst handelt. Diese hatten Zugang zu E-Mails, Chats und einer Vielzahl von Forschungsunterlagen. Es wurden alle Computer der Forschungsabteilung abgerufen und einige Dateien gestohlen.

Auf ähnliche Weise sind im Juli dieses Jahres, insgesamt 19‘252 E-Mails und 8’034 Anhänge des US Democratic National Committee enthüllt worden. Die Sicherheitsfirma behauptet, dass **der Hack die Arbeit von mindestens zwei verschiedenen Gruppen von Hackern ist, die zu russischen Regierungskreisen gehören, deren Ziel es war den republikanischen Kandidaten Donald Trump zu begünstigen.**

Nun, drei Monate vor den US Wahlen hat das FBI den Hack von mindestens zwei Wahldatenbanken durch ausländische Hacker bestätigt und von einer Datenbank wurden tatsächlich Wählerinformationen gestohlen. Die Untersuchungen laufen noch und die IP-Adressen wurden bis nach Russland zurückverfolgt. Zufall?

Um neue Angriffe auf öffentliche Einrichtungen zu verhindern, ist ein gemeinsamer Regulierungs-und Rechtsrahmen erforderlich, dessen Verantwortlichkeiten zwischen den Staaten aufgeteilt werden soll, bilateral oder durch übergeordnete Organisationen.

Ein Jahr ohne Schutz

Systeme des Democratic National Committee für mindestens ein Jahr kompromittiert.

19‘252 E-Mails und 8‘034 Anhänge

des US Democratic National Committee wurden offen gelegt.

Zwei Wahldatenbanken wurden gehackt

durch ausländische Hacker und Wählerinformationen gestohlen.

Änderungen in der Gesetzgebung

Die Revision der Europäischen Datenschutz-Grundverordnung hat auch die Schweiz zu einer – derzeit noch in Überarbeitung – neuen nationalen Datenschutzverordnung veranlasst. Der Anlass für die Änderung der Richtlinien in der EU war die Notwendigkeit, auf die immer stärker werdenden Bedrohungen durch Cyber-Attacken, zu reagieren. Allgemein gab es auch Mangel an Cyber-Security-Experten im Europäischen Raum, welcher weder vom öffentlichen oder privaten Sektor adressiert wurde.

Andere Faktoren, die zur Änderung des Sicherheitsrahmens geführt haben, sind die Tatsachen, dass die Verteidigung eines Landes sich nicht länger auf die Grenzen und die Souveränität beschränkt, sondern auch das Wohl Ihrer Gesellschaft sicherstellen soll, angesichts dieser neuen Risiken.

Ähnlich wie in Deutschland und Österreich regelt das Datenschutzgesetz des Bundes den Datenschutz für die Bundesbehörden und für den privaten Bereich, die Einhaltung des Datenschutzes wird durch den staatlichen Datenschutz- und Öffentlichkeitsbeauftragten kontrolliert. Ein bemerkenswerter Unterschied zu anderen Ländern ist die Tatsache, dass in der Schweiz zusätzlich zur Auskunftspflicht auch eine Informationspflicht besteht (Art.14 u. Art. 18a):

Art. 14 (Bundesgesetz über den Datenschutz vom 19. Juni 1992 „Der Inhaber der Datensammlung ist verpflichtet, die betroffene Person über die Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen profilen zu informieren; diese Informationspflicht gilt auch dann, wenn die Daten bei Dritten beschafft werden. „Ebenso ist diese Informationspflicht für Bundesorgane in Artikel 18 geregelt.

Die Gesetzgebung konzentriert sich hauptsächlich auf den Schutz personenbezogener Daten, in Bezug auf die Verarbeitung dieser Daten, öffentliche Freiheit und die Grundrechte des Einzelnen, und vor allem ihren Ruf und persönliche Privatsphäre und dass ihrer Familie.

In Bezug auf den physischen Speicherort der Daten, bieten Länder innerhalb des Europäischen Wirtschaftsraumes sowie auch der Schweiz ausreichend Sicherheit, und der Datentransfer innerhalb dieser Länder ist rechtlich gesehen keine internationale Übertragung von Daten. Der Europäische Wirtschaftsraum besteht aus den Ländern der Europäischen Union sowie Island, Liechtenstein und Norwegen.

Technology und Gesetzgebung

Das Auftreten neuer Akteure aus unterschiedlichen Bereichen und auch mit unterschiedlichen Motivationen und Fähigkeiten in jeder Sicherheitsdimension zu handeln, behindert die Identifikation der Angreifer und verringert die Fähigkeit der Länder angemessen zu reagieren. Die aktuelle Gesetzgebung ist nicht dynamisch genug um auf die ständigen Veränderungen der Cyber-Kriminalität oder die neuen technologischen und Daten-Management-Anforderungen zu reagieren.

Die im Juli 2016 **veröffentlichten neuen Regeln der EU sollen zur Stärkung im Kampf gegen Cyber-Bedrohungen dienen.** Diese Richtlinien zur Sicherheit von Netz-und Informationssicherheit zielen darauf ab, Standards in der IT-Sicherheit zu erhöhen und die Zusammenarbeit zwischen den Mitgliedstaaten in diesem Bereich zu verbessern. Gleichzeitig gibt es auch neue Regelungen und Verpflichtungen für die Betreiber von grundlegenden Dienstleistungen und kritischen Infrastrukturen (Energie, Verkehr, Gesundheit und Finanzen) sowie für digitale Service Anbieter(Online Marktplätze, Suchmaschinen und Cloud-Dienste).

Laut EU Richtlinie ist nun jeder Staat innerhalb der EU verpflichtet nationale Behörden einzurichten und eine Strategie zur Bekämpfung von Cyber-Bedrohungen zu entwickeln, die in Übereinstimmung mit der EU-Richtlinie liegt und zweifellos eine Überarbeitung der derzeitigen nationalen Cyber-Sicherheitsstrategien verlangt. Ausserdem wird angeregt ein „Netzwerk von Computer-Sicherheitsexperten (Incident Response Team=CSIRT), zu schaffen, dies soll das Vertrauen und die schnelle und effiziente operative Zusammenarbeit unter Mitgliedstaaten fördern.

Ein Beispiel dafür ist, dass die Betreiber von grundlegenden Dienstleistungen verpflichtet sind jeden Vorfall, der eine erhebliche Auswirkung auf die Kontinuität dieser Dienstleitung hat, an die zuständige Behörde oder CSIRT zu melden. In ähnlicher Art und Weise sind Anbieter digital Dienstleistung angehalten Vorfälle, die Ihre Dienstleistung (Online Marktplätze, Suchmaschinen und Cloud-Dienste) erheblich beeinträchtigen, zu melden.

Deshalb ist es wichtig, der neuen EU Verordnung besondere Aufmerksamkeit zu schenken, da sie grossen Einfluss auf die nationalen Standards haben wird.

Cyber-Sicherheitsexperten informieren Regierungen und Bürger über die Wichtigkeit des Schutzes vor Cyber-Attacken und plädieren für eine striktere Umsetzung der Sicherheitsmassnahmen als je zuvor, sollten keine oder nur unzureichende Massnahmen getroffen werden, können die Folgen oft schwerwiegend sein.

Die Lösung zur Anpassung an die stetigen Veränderungen

Die Verwaltungen fördern nun eine Abkehr vom einfachen Modell Cyber-Sicherheit, zu einem mehr umfassenden Sicherheitsmodell basierend auf dem Management der Cyberspace Risiken (Informationssicherung).

Für öffentliche Einrichtungen liegt der Erfolg, zur Gewährsleitung der Cyber-Sicherheit, in der Erfüllung bestimmter Anforderungen:

Echtzeit-Information

Echtzeit-Information über Vorfälle und Sicherheitslücken im Zusammenhang mit Datensicherheit, wie z.B. die zufällige oder illegale Zerstörung, Verlust, Veränderung, unbefugte Offenlegung oder Fernübertragung von Daten.

Datenschutzregulierung

Die Einhaltung von Artikel 35 der “Allgemeinen Datenschutzverordnung” über den Datenschutz mit regelmässiger und systematischer Überwachung von Daten in grossen Mengen

Datenübertragung ins Ausland

Berichterstattung aller möglichen Datenübertragungen in fremde Länder.

Privatsphäre

Verbesserung der individuellen Rechte, darunter das Recht auf Vergessenheit und das Recht auf Datenportabilität.

Schutz

Gewährleistung der Einhaltung der Datenschutzrechte bei Verarbeitung der Daten durch einen Auftragsverarbeiter zur Datenlöschung, Berichterstattung und Meldepflichten sowie der Wartung von Datei-Transfer-Aktivitäten.

Adaptive Defense 360

Im Falle einer elektronischen Verwaltung innerhalb eines Sicherheitsrahmens gibt es bestimmte Anforderungen auf allen Ebenen, sowie die Notwendigkeit verschiedene Technologien zu verwenden um Schwachstellen zu verhindern und gleichzeitig mehrere Verteidigungslinien aufzubauen.

Die Einführung fortschrittlicher Technologien, wie Adaptive Defense, als Ergänzung zu herkömmlichen Antiviren-Lösungen, ermöglicht die Einhaltung der empfohlenen Sicherheitsvorkehrungen und entspricht den technischen Anforderungen und Gesetzgebungen wie oben beschrieben.
Adaptive Defense bietet maximale Sicherheit gegen Bedrohungen und gezielte Attacken auf Unternehmen über 4 grundlegende Säulen:

Visibilität:
Rückverfolgbarkeit und Sichtbarkeit jeder laufenden Aktion.

Erkennung:
Ständige Überwachung aller laufenden Prozesse und Echtzeit-Blockierung von gezielten und Zero-Day-Attacken, sowie anderen fortschrittlichen Bedrohungen. Entwickelt um über traditionelle Antivirus-Lösungen hinauszuwachsen.

Reaktion:
Bereitstellung forensischer Informationen für eine gründliche Analyse eines jeden Angriffsversuchs sowie Werkzeuge zur Fehlerbehebung.

Prävention:
Verhindern zukünftiger Attacken durch Blockieren verdächtiger bzw. nicht als “gut” eingestufter Programme und Verwendung fortgeschrittener Anti-Exploit-Technologie.

panda

Adaptive Defense

Adaptive Defense schützt Computer durch laufende Überwachung und Klassifizierung aller Prozesse auf der Kunden-Infrastruktur und erlaubt nur legale Software. Zusätzlich bietet diese Lösung auch Monitoring-Tools, forensische Analyse und Problemlösung zur Bestimmung des Ausmasses eines verdächtigen Verhaltens und dessen Lösung.

Im Gegensatz zu herkömmlicher Antiviren-Software nutzt **Adaptive Defense ein neues Sicherheitsmodell, das genau auf die spezifische Umgebung des jeweiligen Unternehmens angepasst werden kann,** die Ausführung aller Anwendungen überwacht und kontinuierlich von den Aktionen und Prozessen lernt.

Nach einer kurzen Lernphase ist Adaptive Defense 360 in der Lage Schutzniveaus auf verschiedenste Art und Weise anzubieten, weit über den Fähigkeiten einer herkömmlichen Antiviren-Lösung. Zusätzlich liefert Adaptive Defense wertvolle Informationen über den Kontext, in dem ein Sicherheitsproblem auftritt, so kann der Anwendungsbereich abgegrenzt und effektive Gegenmassnahmen ergriffen werden.

Panda Adaptive Defense 360 ist ein Multi-Plattform-Dienst und unterstützt Windows, Linux, Mac OS X, und Android. Da es in der Cloud gehostet wird, benötigt man für die Administration keine zusätzliche IT-Infrastruktur, so bleiben die Kosten auf einem niedrigen Niveau.

Als Cloud-basierter Sicherheitsdienst liegen die Sicherheitsanforderungen in der direkten Verantwortung des Dienstleisters. **Panda Adaptive Defense ist auf Microsoft's Azure Cloud gehostet.**

Microsoft Azure wurde strengen Tests durch BDO unterzogen, einem unabhängigen Prüfer. BDO bescheinigt, dass die Sicherheitsmassnahmen des Dienstes, sowie jene der IT-Systeme und Anlagen für die Verarbeitung von Daten eine hohe Übereinstimmung mit RD 3/2010 bieten und somit keine weiteren Massnahmen ergriffen werden müssen. **Microsoft ist der erste Hyper-Scale Cloud Services Anbieter, der diese Zertifizierung erhält.**

Abschliessend und unter Berücksichtigung der unterschiedlichen Gesetze zum Datenschutz in den verschiedenen Ländern, ist es wichtig zu betonen, dass Adaptive Defense keine personenbezogenen Daten sammelt und unter keinen Umständen persönliche Daten in die Cloud sendet, damit die Einhaltung aktueller und zukünftiger Datenschutzvorschriften gewährleistet ist.

Schutz gegen fortgeschrittene Bedrohungen und gezielte Angriffe, mit der Fähigkeit abnormales Verhalten zu erkennen. Ein System zur Sicherstellung der Datenvertraulichkeit und Privatsphäre von Information sowie der Wahrung der Vermögenswerte und des Rufs eines Unternehmens. All das ist Adaptive Defense, das einzige fortschrittliche Cyber-Sicherheitssystem, das einen Schutz der nächsten Generation bietet, kombiniert mit modernsten Erkennungs- und Fehlerbehebungstechnologien, die eine Klassifizierung aller laufenden Prozesse ermöglichen.

panda

Adaptive Defense

Mehr Information:

BENELUX
+32 15 45 12 80
belgium@pandasecurity.com

BRAZIL
+55 11 3054-1722
brazil@pandasecurity.com

FRANCE
+33 (0) 1 46842 000
commercial@fr.pandasecurity.com

GERMANY (& AUSTRIA)
+49 (0) 2065 961-0
sales@de.pandasecurity.com

HUNGARY
+36 1 224 03 16
hungary@pandasecurity.com

ITALY
+39 02 24 20 22 08
italy@pandasecurity.com

MEXICO
+52 55 8000 2381
mexico@pandasecurity.com

NORWAY
+47 93 409 300
norway@pandasecurity.com

PORTUGAL
+351 210 414 400
geral@pt.pandasecurity.com

SOUTH AFRICA
+27 21 683 3899
sales@za.pandasecurity.com

SPAIN
+34 900 90 70 80
comercialpanda@pandasecurity.com

SWEDEN (FINLAND & DENMARK)
+46 0850 553 200
sweden@pandasecurity.com

SWITZERLAND
+41 22 994 89 40
info@ch.pandasecurity.com

UNITED KINGDOM
+44 (0) 844 335 3791
sales@uk.pandasecurity.com

USA (& CANADA)
+1 877 263 3881
sales@us.pandasecurity.com

Mehr Information auf:

http://www.pandasecurity.com/switzerland-de/enterprise/solutions/adaptive-defense-360/

oder per Telefon:

+41 22 994 89 40

oder per E-Mail info@ch.pandasecurity.com

panda

Adaptive Defense 360

Uneingeschränkte Transparenz, Absolute Kontrolle

pandasecurity.com

panda