business network communications

CYBER SECURITY & DATENSCHUTZ

IT-Sicherheit – die Herausforderung der Gegenwart und Zukunft in der Schweiz und Europa
Ein E-Paper zu den wichtigsten Fakten rund um die Themen Cyber Security und Datenschutz

INDEX

EINLEITUNG

IT-Sicherheit – die Herausforderung der Gegenwart und Zukunft

Heutzutage ist nahezu alles und jede Person miteinander vernetzt. Dies bietet uns eine Vielzahl an Möglichkeiten, wie zum Beispiel eine schnelle und einfache Kommunikation auf digitalem Weg, das Verwalten von riesigen Datenmengen (Big Data), schnellere Arbeitsprozesse und vieles mehr, von denen wir früher nur träumen konnten. Doch mit den diversen Optionen unseres digitalen Zeitalters gehen auch erhebliche Risiken und mehr Verantwortung einher. Wir bei BNC legen Wert darauf, auch die Schattenseiten der Digitalisierung zu beleuchten und widmen dieses E-Paper dem Thema Cyber Security. Wir haben die wichtigsten Informationen und nützliche Tipps für Ihre IT-Security zusammengefasst.

Zudem haben wir die Meinungen von Rechtsanwalt Dr. iur. Schneider von Walder Wyss Rechtsanwälte – Experte für Rechtsfragen rund um die Themen Informationstechnologie, Datenschutz und Outsourcing – eingeholt.

WAS IST DATENSCHUTZ? WAS IST CYBER SECURITY?

Datenschutz

Der Begriff «Datenschutz» erklärt sich teilweise von allein: Es geht darum, Daten – also Informationen – zu schützen. Das heisst, sie für Unbefugte unzugänglich zu machen und dafür zu sorgen, dass die informationelle Selbstbestimmung des rechtmässigen Besitzers dieser Daten gewährleistet ist. Er muss also jederzeit die Kontrolle über die Aufbewahrung sowie die Verwendung der Daten haben und Änderungen oder Löschungen veranlassen können. Dabei werden nicht nur Informationen über Individuen, sondern auch über juristische Personen – also Firmen – geschützt.

Der Hauptgedanke dabei ist nicht das Schützen der Daten als solche, sondern der Schutz der Persönlichkeit, die sich hinter diesen Daten verbirgt.

In der Schweiz müssen sich Unternehmen an das Bundesgesetz über den Datenschutz (vom 19. Juni 1992) und die entsprechenden Verordnungen sowie an die kantonale Gesetzgebung halten. Seit dem 25. Mai 2018 gilt auf europäischer Ebene zudem die EU-Datenschutz-Grundverordnung (englisch: GDPR «General Data Protection Regulation»). Rechtsanwalt Dr. iur. Schneider von Walder Wyss Rechtsanwälte erläutert, dass mit dieser Verordnung die Datenschutzvorschriften auf europäischer Ebene vereinheitlicht und der Schutz von Personendaten weiter ausgebaut und gestärkt wurden. Ebenso bestehe unter der GDPR ein höheres – wenn nicht sogar ein zu hohes – Sanktionspotenzial für Unternehmen, da der Bussenrahmen erhöht worden ist.

Ferner weist Rechtsanwalt Dr. Schneider darauf hin, dass sich das aktuelle Datenschutzgesetz gegenwärtig in Revision befindet. Mit der Revision werden die Datenschutzvorschriften analog der DSGVO verschärft. Das revidierte Gesetz soll aber nicht vor 2021 in Kraft treten.

Cyber Security

Cyber Security ist eine Erweiterung der klassischen IT-Sicherheit auf den Cyber-Raum. Das heisst, sie ist zuständig für die Nutzersicherheit im Internet und anderen vergleichbaren Netzen. Vor allem in unserer von Digitalisierung geprägten Zeit, in der ein «Internet of Things» (IOT) entsteht bzw. bereits vorhanden ist, Mobilität und Home Office immer wichtiger wird und enorm grosse Datenmengen gespeichert werden, ist eine umfassende Cyber Security unerlässlich. Es gilt mehr denn je, sich vor Datenverlusten und -missbrauch durch Cyberkriminelle zu schützen. Ist es zu einer Attacke oder ähnlichen sicherheitsrelevanten Vorfällen gekommen, sollte dies gemeldet werden, um andere Unternehmen vor Schaden zu bewahren und eine schnelle Problemlösung in Gang zu bringen. Derzeit können Vorfälle und Sicherheitslücken beim Nationalen Zentrum für Cybersicherheit (NCSC) gemeldet werden. Dieses Kompetenzzentrum wurde 2019

WAS IST DATENSCHUTZ? WAS IST CYBER SECURITY?

errichtet und vereint seither die verschiedenen Stellen im Bereich der Cybersicherheit unter einem Dach. Die zentrale «Melde- und Analysestelle Informationssicherung» des Bundes (kurz: MELANI) ist neu ebenfalls an das NCSC angegliedert. Demnächst könnte auch eine Meldepflicht von Sicherheitslücken auf Unternehmen zukommen. Im Rahmen der zweiten nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018-2022 vom 18. April 2018 prüfte der Bund die Einführung einer Meldepflicht von Sicherheitslücken und will bis Ende 2020 über eine Einführung von solchen Pflichten entscheiden.
An den vorangegangenen Ausführungen ist zu erkennen, dass Cyber Security und Datenschutz Hand in Hand gehen. Ist keine adäquate Cyber-Sicherheit aufgebaut, können Unbefugte über das Internet oder andere Netzwerke in Ihre Systeme dringen und an sensible Daten gelangen.
Eine Studie (EN) von KPMG zum Thema Cyber Security (Befragung im Januar 2017) brachte unter anderem folgende Ergebnisse zutage:

1 88 % der befragten Unternehmen gaben an, dass sie in den vergangenen 12 Monaten Opfer einer Cyber-Attacke wurden (ein + von 34 % im Vergleich zum Vorjahr).

2 81 % der Befragten gaben an, in den letzten 12 Monaten ein besseres Bewusstsein für Cyberrisiken gewonnen zu haben.

Diese Ergebnisse und Entwicklungen sind erschreckend und sollten zum Handeln bewegen.

ENTWICKLUNG

Risiken und künftige Herausforderungen

Mit der zunehmenden Digitalisierung, die mittlerweile auch bei kleinen und mittleren Unternehmen angekommen ist und durchaus viele Vorteile wie zum Beispiel die Optimierung von Arbeitsprozessen, Home Office, die Effizienzsteigerung durch eine direkte und schnelle Kommunikation über digitale Kanäle sowie Sparpotenziale (z. B. die Einsparung von Lagerplatz) mit sich bringt, gehen allerdings auch Risiken einher. Die Möglichkeit, sich überall und mit allem vernetzen zu können (IoT), bietet oft auch Unbefugten jederzeit die Möglichkeit, in Systeme einzudringen, sofern diese nicht ausreichend geschützt sind. Bei der Basis sollte angefangen werden. Es ist daher ein umfassender Schutz der IT-Infrastruktur aufzubauen, um das Unternehmen und dessen Reputation sowie Mitarbeitende und Kunden zu schützen. Die Gefahren werden nicht kleiner. Cyberkriminelle entwickeln sich weiter, versuchen auch die neuste Sicherheitssoftware zu überwinden und haben zu oft dabei Erfolg. Daher sind Unternehmen gezwungen, regelmässig Ihre Sicherheitssysteme zu überprüfen, Schwachstellen ausfindig zu machen und gegebenenfalls Anpassungen vorzunehmen. Auf dem neusten Stand bleiben heisst also die Devise! Auch auf politischer Seite wurde diesbezüglich ein Handlungsbedarf erkannt. Im Rahmen der zweiten Nationalen Strategie zu Cyber-Risiken (NCS) hat der Bund für die Jahre 2018-2022 über weitere Ziele beschlossen. So sollen Kompetenzen und spezifisches Know-How weiter ausgebaut werden, die internationale Kooperation in diesem Bereich gefördert und die Massnahmen der Cyber-Abwehr durch die Armee und den Nachrichtendienst des Bundes (NDB) verstärkt werden. Zudem wurde der Bund wie erwähnt beauftragt, in Zusammenarbeit mit der Wirtschaft Mindeststandards für die Cyber-Sicherheit zu entwickeln und die Einführung von Meldepflichten für Cyber-Vorfälle zu prüfen.

ENTWICKLUNG

Risiken

Es werden täglich viele Daten gesammelt: über Kunden, Unternehmen, technische Details, Verfahren, Mitarbeitende etc. Wenn Cyberkriminelle an diese teilweise sehr sensiblen Daten herankommen, kann das schwerwiegende Folgen wie beispielsweise Daten- und Identitätsdiebstahl oder Erpressung haben.

Zu den aktuellen Gefahren gehören:

- **Schadsoftware (auch «Malware» genannt) in E-Mails:** Sie befindet sich meistens in den Anhängen, aber auch das Anklicken von Links unseriöser E-Mails kann zur Installation von Malware auf dem Endgerät führen. Wenn eine Schadsoftware heruntergeladen wurde, kann sie sich sehr schnell verbreiten, Daten auf dem Endgerät zerstören, das infizierte Gerät für Spamversand missbrauchen, persönlichen Dateien und Daten stehlen oder E-Banking Betrug auslösen.
- **Schadsoftware auf Webseiten:** Diese kann durch das Besuchen bestimmter Webseiten, auf die man oft durch unseriöse E-Mails verlinkt wird, installiert werden.
- **Phishing:** Der Begriff bezeichnet die Betrugsmasche, sich per E-Mail vertrauliche Daten von ahnungslosen und gutgläubigen Nutzern zu erschwindeln. Dabei fälscht der Absendende Identitäten, um seriös zu erscheinen. E-Mails und deren Herkunft sollten also stets kritisch hinterfragt werden. Bei einer seriösen Herkunft wird in der Regel nicht verlangt, vertrauliche Daten preiszugeben.

ENTWICKLUNG

- **Social Engineering:** Bei dieser Betrugsmasche geht es den Angreifenden ebenfalls darum, an vertrauliche Daten der Opfer zu gelangen. Bei dieser Methode geben sich die Betrüger als Systemadministrator oder Sicherheitsverantwortliche eines Unternehmens aus und geben vor, bei der Lösung erfundener Probleme helfen zu wollen. Dafür brauchen sie natürlich die vertraulichen Daten wie z. B. Kontodaten oder Zugangsdaten zu Systemen.
- **DDoS Attacken (Distributed Denial of Service):** Diese Attacken sind gezielte Angriffe auf ein System mit dem Ziel, dieses zu stören oder lahmzulegen. Dabei erfolgen viele Angriffe (oft in Form von Anfragen), die von einem Angreifenden ferngesteuert werden.
- **Verschlüsselungstrojaner:** Sie gehören zur Familie der Malware. Sie werden auch «Erpressungstrojaner» genannt, da sie Daten verschlüsseln und diese erst freigegeben werden, wenn der Nutzer einen bestimmten Betrag i. d. R. in Bitcoins zahlt.

Diese Gefahren zeigen den enormen Handlungsspielraum der Cyberkriminellen auf. Über verschiedene Kanäle können sie erheblichen Schaden anrichten. Zudem können neue Technologien und Möglichkeiten wie beispielsweise BYOD (Bring Your Own Device) oder Mobile Devices die Cyber-Sicherheit und den Datenschutz zusätzlich erheblich beeinträchtigen und führen oft zu Kompromissen zuungunsten der Datenbesitzenden. Sehr oft stellen auch ungeschulte Mitarbeitende ein Risiko dar, indem sie beispielsweise ahnungslos eine unseriöse und gefährliche E-Mail öffnen. Mitarbeitende sind so gut vorbereitet, wie das Management dies ermöglicht und führt. Es gibt hier immer Verbesserungspotenzial, aber in vielen Firmen in der Schweiz ist das Sicherheitsbewusstsein hoch. Jedoch wissen dies auch die Angreifenden und verfeinern ihre Methoden (z. B. «Social Engineering» usw.) auch immer weiter.
Unternehmen müssen sich ihrer Verantwortung, sensible Daten zu schützen und den potenziellen Gefahren bewusst sein, um angemessen handeln und eine adäquate IT-Security aufbauen zu können.

ENTWICKLUNG

Es wird mehr Angriffe bekannter Bauart geben, bei denen in grosser Menge nach «Zufallsopfern» gesucht wird. Parallel dazu werden Firmen, Infrastrukturen und exponierte Personen zunehmend gezielt unterwegs oder auch zu Hause angegriffen. Schliesslich müssen sich auch der Staat und das Militär noch stärker als bisher mit Cyber-Angriffen auseinandersetzen bzw. auf entsprechende Angriffsversuche vorbereitet sein.

Sicherheitstechnologien in den Schweizer Unternehmen nach Sektor, 2015

In % Anteilen aller Firmen

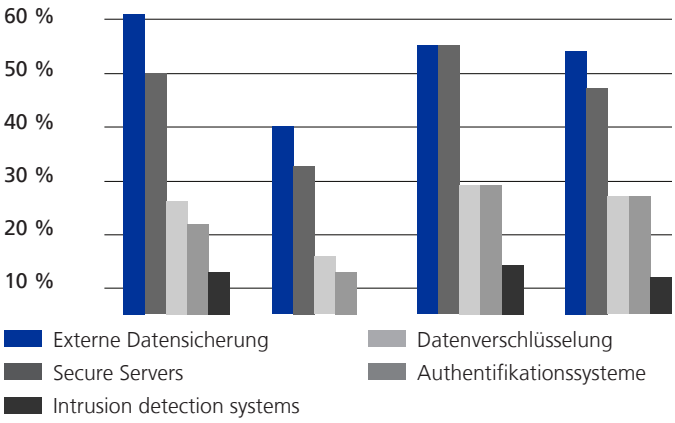

Diagramm 1: Sicherheitstechnologien in Schweizer Unternehmen nach Sektoren

Quelle: Bundesamt für Statistik Schweiz

Herausforderungen

In einer Studie des IT-Research- und Beratungsunternehmens Gartner wurden vier Faktoren identifiziert, die den Markt für Security-Software verändern: die zunehmende Nutzung von Advanced Analytics, grössere IT-Ökosysteme, wachsende Akzeptanz von Software as a Service (SaaS) und die Aussicht auf strengere Regulierung sowie drohende Strafen. Neben diesen Faktoren kann auch die zunehmende Auslagerung von IT- und Netzinfrastrukturen ohne das Auslagern der zugehörigen Sicherheitsfunktionen sehr kritisch sein. Des Weiteren zählt fehlendes Know-how zur Evaluation und zum Selbsteinsatz von Sicherheitslösungen sowie das mangelnde Management-Verständnis für komplexe Sicherheits- und Risikobeurteilungen einiger Firmen zu den kritischen Faktoren, die die IT-Security stark beeinflussen.

Im Diagramm 1 ist deutlich zu erkennen, dass zunehmend IT-Infrastrukturen ausgelagert werden.

ENTWICKLUNG

Die externe Datensicherung ist sehr beliebt. Doch sind die Daten extern auch ausreichend geschützt? Wenn Unternehmen zum Beispiel Cloud-Computing betreiben und Daten in der Cloud abgelegt werden, muss natürlich eine adäquate Cloud-Security eingerichtet werden. Bei Cloud-Computing werden IT-Infrastrukturen wie zum Beispiel Rechenleistung, Software und Speicherplatz über das Internet genutzt. Eine besondere Herausforderung ist dabei das Sichern der Cloud, um Unbefugten keinen Zugang zu den Daten zu ermöglichen. Cloud-Lösungen sind vor allem für «Big Data» sehr praktisch. Unter diesem Begriff versteht man Datenmengen, die sehr komplex, gross, schnelllebig und oft auch schlecht strukturiert sind. Sie benötigen sehr viel Speicherkapazität, die man durch eine Cloud-Lösung leicht bekommen kann. Auch «Infrastructure as a Service» (IaaS) ist über eine Cloud möglich. Bei diesem Modell wird Rechenleistung ganz nach Bedarf gemietet. Dieser Service bringt eine Reihe von Vorteilen mit sich. So können zum Beispiel Belastungsspitzen abgefangen, Grössenveränderungen der Systeme vorgenommen und Kapazitäten schnell freigegeben werden, wenn diese nicht benötigt werden. Alle Systeme und Daten der Cloud müssen dabei unbedingt umfassend geschützt sein.
Des Weiteren zeigt das Diagramm, dass die Sicherheitstechnologie sehr abhängig von den Sektoren ist. Industrie und Dienstleistungsunternehmen haben oft sehr viele sensible Daten gespeichert und sind daher besonders in der Pflicht, diese Daten zu schützen.

In einer Studie von PwC Schweiz, der Google Switzerland GmbH und digitalswitzerland prognostizieren 76 % der befragten KMU, dass die Digitalisierung den Markt in den nächsten fünf Jahren grundlegend verändern werde. Momentan sind KMU aufgrund der verbreiteten Einstellung getreu dem Motto «wir sind zu klein, um Opfer einer Cyber-Attacke zu werden» besonders gefährdet. Sie sparen oft an der falschen Stelle – bei den Sicherheitsmassnahmen – womit sie geradezu prädestiniert sind, Opfer eines Cyber-Angriffs zu werden. KMU haben einen besonderen Handlungsbedarf in Sachen Cyber Security und Datenschutz, da sie oft nicht die nötigen eigenen Ressourcen haben und andererseits aufgrund ihrer knappen Ressourcendecke die Folgen eines erfolgreichen Angriffs (z. B. Verlust von geistigem Eigentum oder Rufschädigung) nicht kompensieren können.

TIPPS

Nützliche Tipps für jedes Unternehmen

Im Folgenden haben wir kurz die wichtigsten Tipps/Aspekte zu den Themen Datenschutz, Cyber-Attacken und GDPR zusammengefasst.

Sechs Wege Ihre Daten besser zu schützen

- unternehmensspezifsche Anforderungen klar defnieren (z. B. rollenbasierte Zugänge zu IT-Systemen)
- auf Hilfsmittel wie Datenklassifkation zurückgreifen
- evtl. einen Datenschutzbeauftragten bestimmen, der sich auf dem neusten Stand hält und gegebenenfalls Anpassungen vornimmt
- Firewalls auch in Cloud-Umgebungen installieren und das Netzwerk angemessen zonieren
- Antivirusprogramme flächendeckend ausrollen (sollten Teil eines grösseren Abwehr-Dispositivs sein)
- Mitarbeitende schulen bzw. für Cyber Security und Datenschutz sensibilisieren

Was ist für Unternehmen zur GDPR zu beachten

- Es ist zu prüfen, welche Regelungen der Verordnung Ihr Unternehmen betreffen. Wenn nötig, sollten Anpassungen an Arbeitsprozessen etc. vorgenommen werden.
- Die GDPR ist für einige Unternehmen mit Kosten und beträchtlichen zeitlichen Umfang verbunden.
- Es ist sorgfältig zu prüfen, unter welchen Umständen die GDRP für Sie gilt.
- Die Anwendung muss parallel zu nationalen Datenschutzgesetzen praktisch erprobt werden.

TIPPS

Dr. iur. Schneider empfiehlt folgendes Handeln bei einer Cyber-Attacke

- befallene Systeme von Netz trennen
- durch Gegenmassnahmen (z. B. Abschalten betroffener Systeme) Ausbreitung auf weitere Rechner innerhalb des internen Netzwerks verhindern
- Wiederherstellung der Daten
- Massnahmen gegen die Ausbreitung auf externe Systeme durchführen (z. B. Systeme vom Internet trennen)
- überprüfen, ob Informationspflichten bestehen (zum Beispiel an Vertragspartner, Behörden und/oder betroffene Personen)
- bei Erpressungsversuchen von Cyberkriminellen nicht bezahlen
- allenfalls Benachrichtigung des NCSC oder einer diesem angegliederten Kompetenzstellen (MELANI, Computer Emergency Response Team (CERTs), Fachstelle für die IKT-Sicherheit des Bundes)
- Dokumentationen von NCSC berücksichtigen
- interne und externe Kommunikation im Voraus regeln
- interne Zuständigkeiten, Stellvertretungen und Eskalation vorab klären

TIPPS

Schweizer Firmen sollten in Sachen Cyber Security auf Folgendes achten

- abwehren, was mit vernünftigem Ressourceneinsatz abzuwehren ist
- rasch erkennen und handeln können, wenn ein Angriff erfolgreich sein könnte
- «Plan B», um den Angriff zu überstehen und wieder in den Normalbetrieb zu kommen
- systematischer Verbesserungsprozess, um aus allfälligen Fehlern zu lernen
- gute Vernetzung mit Stellen, die ggf. helfen können (insbesondere die verschiedenen Kompetenzstellen des NCSC, wie MELANI, Computer Emergency Response Team (CERTs), Fachstelle für die IKT-Sicherheit des Bundes usw.)

Wenn ein Unternehmen Opfer einer Cyber-Attacke geworden ist, muss der Fall zur Anzeige gebracht werden. Nur dadurch entsteht eine abschreckende Wirkung, wie auch ein vollständigeres Lagebild.

FAZIT

Wie die vorangegangenen Ausführungen deutlich gemacht haben, stellen Cyber Security und Datenschutz grosse Herausforderungen für Unternehmen dar, denen sie sich stellen müssen. Sowohl nationale als auch europäische und internationale Regelungen müssen je nach Unternehmen berücksichtigt werden. Dabei ist es unerlässlich, sich regelmässig auf dem neusten Stand zu halten, um keine Datenschutzverletzungen zu begehen.

Schützen Sie sich, Ihr Unternehmen, dessen Mitarbeitende und Kunden mit einer umfassenden Cyber Security vor Cyberkriminellen. Es kommen immer mehr Risiken auf uns zu, denn die Welt der Cyberkriminalität entwickelt sich stets weiter. Auch neue Technologien und künftige Herausforderungen, die sich schon erahnen lassen, müssen in ein IT-Sicherheitskonzept einbezogen werden. Unsere IT-Experten stehen Ihnen von der Planung bis hin zur technischen Realisierung bei der Bewältigung dieser Aufgaben zur Seite.

Ihr Kontakt

Gerne beantworten wir Ihre Fragen persönlich.

Martin Buck
Head of Competence Center Security
Tel. +41 44 503 58 08
martin.buck@bnc.ch
www.bnc.ch

FAZIT

Unser Service

Die IT-Experten von BNC unterstützen Sie dabei, eine zukunftsorientierte und unternehmensgerechte IT-Security aufzubauen. Seit dem Jahr 2000 arbeiteten wir bei BNC mit unserem Technologiepartner Check Point – einem Marktführer in Sachen Cyber Security – zusammen. Mit den umfassenden Security Lösungen von Check Point implementieren wir Ihnen eine Sicherheitsstruktur, die auch kommenden Herausforderungen standhält.

Starten Sie hier den Instant Security Check.

Hier finden Sie eine Auswahl unserer Security Dienstleistungen:

- BNC Security Checkup
- BNC Netzwerk Zonenkonzept
- BNC Verwundbarkeitsanalyse

IMPRESSUM

Herausgeber
BNC Business Network
Communications AG
Grubenstrasse 7b | Postfach
3322 Urtenen-Schönbühl

Phone: +41 31 858 58 58

marketing@bnc.ch

Erschienen am 1. April 2020

business network communications