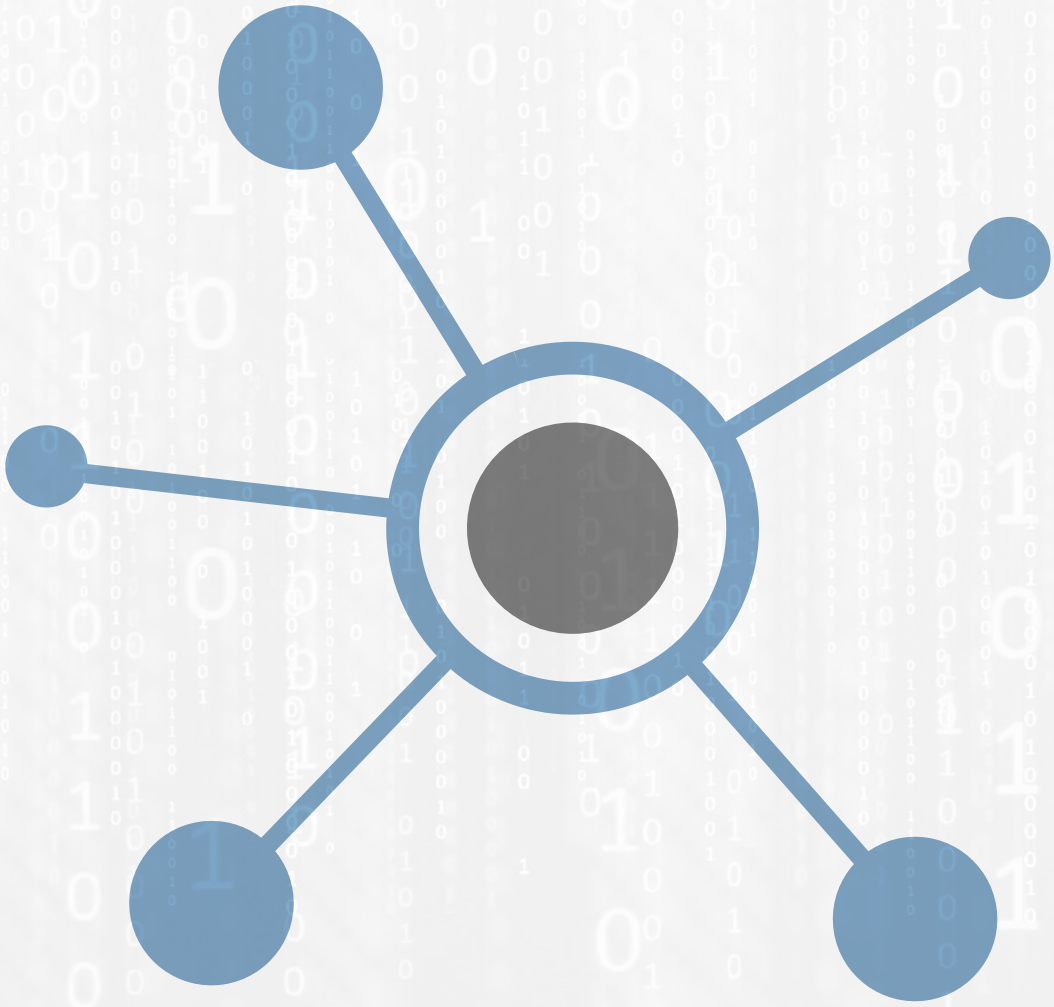
Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

Die Digitale Transformation und Network Security

Marc K. Peter, Corin Kraft & Fabienne Laubscher

Arbeitsbericht 10.2018
Think Tank Digitale Transformation



Partner:

business network communications

aruba
a Hewlett Packard Enterprise company

Die Digitale Transformation
und Network Security

Einleitung und Diskussionspunkte

In der Think Tank-Reihe der FHNW Hochschule für Wirtschaft zur Digitalen Transformation erhalten die Teilnehmenden aktuelle und relevante Informationen zum Stand der Digitalen Transformation in der Schweiz. Als Basis dient die umfangreiche FHNW HSW-Studie (Peter, 2017) mit über 2'500 Befragten. Die Studie zeigt, wo und wie Schweizer Firmen heute und zukünftig investieren.

Der Think Tank vom 13. September 2018 behandelte das Thema Netzwerksicherheit im Zusammenhang mit der Digitalen Transformation. Nach der Präsentation der Studienresultate und wichtiger Modelle diskutierten die Teilnehmenden zentrale Aspekte der Cyber- und Netzwerksicherheit – inklusive aktuellen Problemstellungen und Lösungsansätzen. Die Diskussionsresultate wurden im vorliegenden Bericht zusammengefasst und publiziert.

Die Teilnehmenden des Think Tank der FHNW Hochschule für Wirtschaft und BNC diskutierten die folgenden Fragen:

- Wie erleben Sie die Digitale Transformation?
- Investieren Sie aktiv in die Cyber- und Netzwerksicherheit?
- Nutzen Sie Network Access Control (NAC) und/oder Intrusion Detection Systems (IDS)?

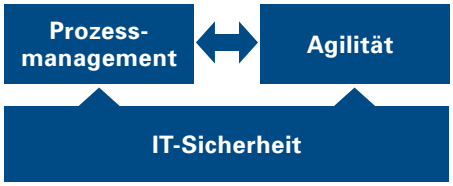


Abbildung 1: Die Spannungsfelder der Digitalen Transformation (FHNW-HSW Think Tank).

Die Digitale Transformation und Informationstechnologien (IT)

Eingangs wurde darüber diskutiert, ob es sich bei der Digitalen Transformation nur um einen Hype handelt, welcher im Kern eigentlich ein IT-Projekt ist. Relativ schnell zeichnet sich ab, dass neben der IT auch Themen wie Big Data und Prozessmanagement wichtige Rollen einnehmen, obwohl das klassische Prozessmanagement in vielen Firmen nicht mehr unterstützt wird, sondern der Fokus auf Agilität gesetzt wird (Daniel Lörtscher, EWB). Abkürzungen und Vereinfachungen sowie die Zusammenarbeit mit externen Partnern werden gesucht. Zudem entsteht in vielen Unternehmen eine «Schatten-IT»: Die vielen, teils unkoordinierten, IT-Projekte «schiessen wie Pilze aus dem Boden». Eric von Ah (Ammann Group) präzisiert, dass Agilität heute ein «Muss» ist, getrieben vom stetigen Wandel und neuen IT-Projekten. Mit neuen Technologien und dem konstanten Wandel entwickeln sich neue Gesellschaftsnormen, welche auch von den Unternehmen berücksichtigt werden müssen.

Die Teilnehmenden sind sich einig, dass die meisten IT-Projekte im Umfeld der Digitalen Transformation marktgetrieben sind. Die technische Umsetzung ist in vielen Fällen weiter fortgeschritten als die interne Prozessabbildung. In anderen Worten: neue Ideen kollidieren mit alten Strukturen und Innovation stösst an die Grenzen der etablierten Prozesse eines Unternehmens. In den letzten zehn Jahren wurden die Mitarbeitenden aus Gründen der Sicherheit, Transparenz und Nachvollziehbarkeit jedoch genau auf die Einhaltung dieser Prozesse getrimmt. Gleichzeitig gilt es, in Richtung Agilität umzudenken, damit Innovation nicht an starren Prozessen scheitert.

An dieser Stelle entsteht die Frage, ob die Aufgaben der IT als Dienstleisterin oder Innovatorin wahrgenommen werden sollten (Andreas Stern, Walo und Dominik Dätwyler, Müller-Steinag). Zudem wird das Investitionsvolumen in IT-Lösungen eher steigen, als dass diese IT-Investitionen im Zusammenhang mit der Unternehmenstransformation zu direkten Einsparungen führen.

Im Spannungsfeld von Prozessmanagement und Agilität (Abbildung 1) wird schlussendlich die Frage nach der Notwendigkeit der Digitalen Transformation diskutiert. Dabei kommen die Treiber für Transformationsprojekte zur Sprache: Wachstums- und Innovationsdruck der Unternehmen, neue Kundenanforderungen und der stetig wachsende Wettbewerbsdruck.

Umsetzung von IT-Projekten im Umfeld der Unternehmenskultur

Roman Feierabend (isolutions) führt an, dass die vielfach zitierten Beispiele von Uber® und Airbnb® zwar interessant sind, diese aber wenig Grundlage für die Unternehmenstransformation für die Schweizer KMU (z.B. einer Schreinerei) geben würden – für diese ist die Digitale Transformation viel schwieriger nachvollziehbar. Es bedarf also unbedingt einer Veranschaulichung für KMU. Die Digitale Transformation ist getrieben von neuen Technologien: Jedoch wird ein grosser Teil der Kosten, die bei der Einführung dieser neuen Technologien entstehen, gar nicht für die IT eingesetzt, sondern für Begleitprojekte zum eigentlichen Projekt. Damit wird der Kulturwandel, getrieben von den neuen Technologien, erfolgreich(er) umgesetzt.

Neben dem für die erfolgreiche Transformation notwendigen Kulturwandel müssen Unternehmen auch in die Weiterbildung investieren. Hier wurde angemerkt, dass die klassischen Schulungen (Mitarbeitende versammeln sich in einem Klassenzimmer und werden von einer Fachperson geschult) nicht mehr erfolgreich sind. Viel mehr sind Selbstbedienungsportale gefragt, z.B. in Form von Tutorial Videos oder Webinars. Eric von Ah schliesst die Diskussion mit der Aussage ab, dass der Kulturwandel letzten Endes mit der persönlichen Einstellung und Neugierde der Mitarbeitenden zusammenhängt.

Mobile Access? Wired vs. Wireless LAN

In einem Teilaspekt der Diskussion wurde der Frage nachgegangen, ob Unternehmen heute im Zug der Unternehmenstransformation auf Wired oder Wireless LAN setzen.

Im Grundsatz setzen die Unternehmen heute auf die Strategie «Mobile First», was Bernhard Leutwiler (BNC) bekräftigt: Die Geräte werden also via Wireless Accesspoints verbunden, wobei multifunktionale Geräte mit Kabel (wired) verbunden ins Netz angeschlossen werden.

Die Teilnehmenden sind sich einig, dass es mit Wireless Access keine negativen Punkte gibt und eine breite Möglichkeit von Sicherheitskonfigurationen bei Wireless möglich sind. Daniel Lörtscher (EWB) schildert den Neubau eines Gebäudes, in welchem konsequent auf «Mobile First» gesetzt wird. Generell bestätigen die Teilnehmenden, dass ein Neubezug oder die Renovation eines Gebäudes sowie die Umstellung auf die Arbeitsweise «Shared Desk» oft als Anlass genutzt wird, um auf Wireless umzustellen. Helmut Schneider (UKBB) erklärt, dass es mit Wireless LAN diverse neue Anwendungspotenziale gibt, so z.B. die mobile Visite bei Patientenbesuchen.

Die IT-Sicherheit in Schweizer Unternehmen

Das Thema IT-Sicherheit ist bei der Hälfte der teilnehmenden Unternehmen auf der Stufe Geschäftsleitung angekommen. Jedoch nur bei etwa einem Drittel der teilnehmenden Unternehmen gibt es eine explizite Fachperson, welche für den Bereich IT-Sicherheit verantwortlich ist. Ein SOC-Team (Security Operations Center) ist sogar nur bei zwei teilnehmenden Unternehmen vorhanden. In der Diskussion wird klar, dass das Thema (noch) nicht für alle Unternehmen den gleichen Stellenwert hat. Ein Teilnehmer wundert sich, ob denn nun wirklich alle KMU in IT-Sicherheitsmassnahmen investieren müssen («Weshalb sollen wir uns als KMU hier allzu grosse Sorgen machen? Welche Informationen generieren wir denn überhaupt, die für andere interessant sein könnten?»).

Treiber für den Bedarf einer guter IT-Sicherheit ist nicht nur der Schutz von Unternehmensdaten, sondern gerade der Schutz der Kundendaten, um die eigenen Kundinnen und Kunden zu schützen. Ein Beispiel wird genannt, wo ein Unternehmen seine Daten klassifiziert hat, um anschliessend die notwendigen IT-Sicherheitsmassnahmen zu planen. Die Datenschutz-Grundverordnung (DSGVO bzw. GDPR) hätte Unternehmen dabei geholfen, das Thema der Datensicherheit («Welche Daten haben wir?» «Wie werden diese genutzt?») überhaupt einmal anzugehen.

Im Folgenden werden diverse Szenarien und Probleme mit der IT-Sicherheit diskutiert, wie z.B. der Fall einer Mitarbeiterin, welche eine private externe Festplatte an ihrem Geschäftscomputer angeschlossen hatte. Auf dieser Festplatte wurde durch aktives Scannen ein Keylogger (Programm zur illegalen Erfassung der Usereingaben) entdeckt.

Abschliessend sind sich die Teilnehmenden einig, dass IT-Sicherheitslösungen alleine noch keinen Schutz bieten. Der Risikofaktor Mensch ist eine schwierig zu kontrollierende Komponente in Sicherheitsangelegenheiten und kann eigentlich fast nur durch Schulungen und die Sensibilisierung der Mitarbeitenden reduziert werden. Ebenfalls notwendig sind personelle Ressourcen, um den Problemen nachzugehen: «Die Lösungen müssen auch bewirtschaftet werden können». Sind diese Ressourcen nicht vorhanden, wird mit der Implementierung einer IT-Sicherheitslösung je nachdem sogar eine falsche Sicherheit suggeriert.

Cyber- und Netzwerk-Sicherheit

Ein Experte stellt fest: «Wir sind uns bewusst, dass wir bereits kompromittiert sein könnten. Die Frage ist viel mehr, wie ein Unternehmen dies bemerkt und was dagegen getan werden kann». Bezüglich IT-Sicherheitslösungen kann der Think Tank in drei Gruppen eingeteilt werden: eine Gruppe verfügt über keine IT-Sicherheitslösungen (NAC, IDS), eine Gruppe ist auf Stufe IDS aktiv und nur die dritte, kleinere Gruppe hat die Möglichkeit, auf NAC-Lösungen zuzugreifen, obwohl der Bedarf an solchen Lösungen bei den meisten Teilnehmenden vorhanden ist. Die Unternehmen in der zweiten Gruppe, die Mehrheit der Teilnehmenden, verfügen über Systeme, welche Anomalien identifizieren. Es herrscht jedoch Konsens, dass viel Potenzial für bessere Monitoring- und Analyselösungen (z.B. mittels Dashboards und Alerting) bestehen. Ein Teilnehmer sagt, dass «…[sie] in den unteren Layern (Schichten) gut bedient sind, aber in den oberen Layern überhaupt nicht». Ein Teilnehmer schildert den Fall, wie gerade Online-Bewerbungen von potenziellen neuen Mitarbeitenden, welche Links zu externen Plattformen mit Bewerbungsdossier enthalten, zum Risiko werden. Die Personalverantwortlichen müssen geschult werden, um Zugangs- und Datenmanagementrichtlinien zu befolgen, mögliche Risikofaktoren zu erkennen und entsprechend zu reagieren.

In vielen Unternehmen werden der Datenverkehr und die Zugriffszeiten der Mitarbeitenden nicht durch Network Access Control (NAC) und/oder Intrusion Detection Systems (IDS) überwacht. Mit diesen Lösungen wird versucht, Anomalien festzustellen. So wird zum Beispiel die illegale Übermittlung von Unternehmensdaten durch Hacker vermieden, welche die Zugangsdaten von Mitarbeitenden stehlen und dann nutzen.

Bei der Applikationssicherheit veranlasst ein teilnehmendes Unternehmen bei der Einführung jeweils ein Audit, um die App zu zertifizieren, bevor diese in Betrieb genommen werden darf. Rund die Hälfte aller teilnehmenden Unternehmen führt regelmässig Audits durch. Dabei sind sich die Experten einig, dass einmalige Audits problematisch sind, weil auch diese ein falsches Sicherheitsgefühl provozieren könnten. Viel wichtiger wäre ein laufender, aktiver Scan, um Schwachstellen in der Infrastruktur zu identifizieren und stetig zu verbessern.

Die Teilnehmenden bestätigten den Bedarf nach einer gesamtheitlichen Sicherheitslösung, bestehend aus NAC und IDS, welche in Form eines SOC als «Managed Service» angeboten werden könnte. Dies unterstützt Unternehmen dabei, laufend Schwachstellenscans durchzuführen und sichert die durchgehende Verfügbarkeit von IT-Sicherheitsmitarbeitenden (24/7) mit dem notwendigen Spezialwissen.

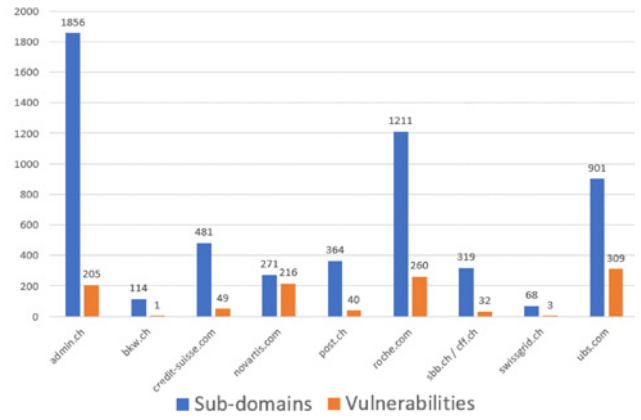


Abbildung 2: Cyber-Schwachstellen aufgrund eines IP-/Domainscans bei ausgewählten Schweizer Unternehmen (Cyobs, Juli 2018).

Zusammenfassung und Empfehlung

Die Teilnehmenden des Think Tank haben festgestellt, dass die meisten IT-Projekte rund um die Digitale Transformation marktgetrieben sind. Dabei befinden sich Unternehmen im Spannungsfeld zwischen Prozessmanagement, Agilität und IT-Sicherheit. Um mit diesem Spannungsfeld umzugehen, bedarf es einer Auseinandersetzung auf Stufe Geschäftsleitung.

Es ergeben sich folgende Handlungsempfehlungen:

- Die Schulung und Sensibilisierung der Mitarbeitenden sowie der Aufbau und Betrieb von Firewalls, die Einführung einer NAC-Lösung und im besten Fall eines SOC.
- Prozesse und Regeln sollen definiert und implementiert werden, um die Schatten-IT in Unternehmen zu steuern bzw. zu reduzieren.
- Neue IT-Projekte bieten eine Chance, um den Kulturwandel in Unternehmen voranzutreiben. Hier empfiehlt es sich, alternative und innovative Schulungsformen anzubieten.
- «Mobile First» ist der bevorzugte Ansatz, um Netzwerk-Access in Unternehmen zur Verfügung zu stellen.
- Die neue Datenschutz-Grundverordnung (DSGVO bzw. GDPR) gibt Unternehmen den Anstoss, ihre Daten zu klassifizieren und entsprechende IT-Sicherheitsmassnahmen zu definieren und zu implementieren.
- Das Thema IT-Sicherheit bewegt Unternehmen: für KMU sind die hierfür notwendigen Budgets nicht immer verfügbar, während dem das Thema bei grösseren Unternehmen auf Stufe CEO/Geschäftsleitung angekommen ist.
- IT-Sicherheitslösungen existieren bei der Mehrheit der teilnehmenden Unternehmen und der Bedarf nach Monitoring- und Analysefähigkeiten ist hoch.
- Neben den klassischen Ansätzen (IDS, NAC) wünschen sich die Unternehmen einen ganzheitlicheren Ansatz (z.B. mittels SOC), um Schwachstellenscans laufend durchzuführen und um in einem Managed Services Modell auf die Ressourcen des Partners/der Partnerin zugreifen zu können.
- IT-Sicherheitslösungen alleine bieten noch keinen Schutz: Unternehmen benötigen weiter personelle Ressourcen, damit die Lösungen auch bewirtschaftet werden können.

Der Think Tank

BNC Business Network Communications und Aruba sowie das Zentrum für Digitale Transformation der FHNW Hochschule für Wirtschaft luden am 13. September 2018 ausgewählte Unternehmen zum Think Tank in Olten ein.

Ziel der Think Tank-Reihe ist es, aktuelle Themen rund um die Digitale Transformation zu diskutieren und Gedankenanstösse aus der Wirtschaft in die wissenschaftliche Forschung zu übertragen.

Die FHNW Hochschule für Wirtschaft unterstützt, unter der Leitung von Prof. Dr. Marc K. Peter, die Veranstaltung fachlich und publiziert den Bericht des Think Tank.

Teilnehmende des Think Tank:

Martin Buck	Sales Director Zürich BNC Business Network Communications AG
Dominik Dätwyler	CIO, MÜLLER-STEINAG Gruppe
Roman Feierabend	Head of Managed Services, isolutions
Corin Kraft	Projektleiterin und wissenschaftliche Mitarbeiterin, FHNW Hochschule für Wirtschaft
Andreas Klopfenstein	Projektleiter Netzwerk & Security, BLS Netz AG
Bernhard Leutwiler	Head of Managed Services, BNC Business Network Communications AG
Daniel Lörtscher	Leiter IT, EWB Energie Wasser Bern
Helmut Schneider	Leiter ICT, UKBB Universitäts-Kinderspital beider Basel
Olivier Schrämmli	Stv. Leiter IT, Einwohnergemeinde Olten
Andreas Stern	Netzwerkverantwortlicher, Walo Bertschinger AG
Peter Wielath	Head Core Platforms, Bank Vontobel AG
Marc K. Peter	Leiter Zentrum für Digitale Transformation, FHNW Hochschule für Wirtschaft
Eric von Ah	Global Operations Manager, Ammann Schweiz AG

Quellen:

Cyobs 2018 (Juli): *Cyber-Daten aus der Schweiz und dem Ausland.* Dreamlab Technologies AG, Bern (www.cyobs.ch).

Peter, Marc K. (Hrsg.) 2017: *KMU-Transformation: Als KMU die Digitale Transformation erfolgreich umsetzen. Forschungsresultate und Praxisleitfaden.* FHNW Hochschule für Wirtschaft, Olten.

Kontakt:

Prof. Dr. Marc K. Peter, FHNW Hochschule für Wirtschaft
marc.peter@fhnw.ch

www.fhnw.ch/wirtschaft
www.kmu-transformation.ch

Corin Kraft, FHNW Hochschule für Wirtschaft
corin.kraft@fhnw.ch

Fabienne Laubscher, BNC Business Network Communications AG
fabienne.laubscher@bnc.ch