Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

Analyse und Sensibilisierung IT-Sicherheit

Workshops IT-Sicherheit und Analyse der öffentlichen Angriffsfläche

TITAN-E Projet Européen

Marc K. Peter, Konstanze Schäfer, Anna V. Rozumowski,
Jacek Jonczy und Mischa Obrecht

trinational-digital-business.net

TITAN-E

Impressum

Marc K. Peter, Konstanze Schäfer, Anna V. Rozumowski,
Jacek Jonczy und Mischa Obrecht:
Analyse und Sensibilisierung IT-Sicherheit
Workshops IT-Sicherheit und Analyse der öffentlichen Angriffsfläche
TITAN-E Projet Européen
Hochschule für Wirtschaft FHNW
Olten, Juli 2023

Dieses Werk wurde sorgfältig erarbeitet. Dennoch übernehmen Autorinnen/Autoren und die beteiligten Forschungspartnerinnen/-partner in keinem Fall, einschliesslich des vorliegenden Werkes, irgendeine Haftung für die Richtigkeit von Angaben, Hinweisen und Ratschlägen sowie für eventuelle Druckfehler.

Alle Rechte, auch die Übersetzung in andere Sprachen, vorbehalten.

Kein Teil dieses Werkes darf ohne schriftliche Genehmigung der Autorinnen/Autoren in irgendeiner Form reproduziert oder in eine von Maschinen, insbesondere von Datenverarbeitungsmaschinen, verwendbare Sprache übertragen und/oder übersetzt werden.

Die Rechte der genannten Marken liegen bei ihren entsprechenden Eigentümern.

Koordination dieser Publikation: Konstanze Schäfer,
Dreamlab Technologies, und Prof. Dr. Marc K. Peter, Hochschule für Wirtschaft FHNW

Inhalt

Zum Projekt **4**
Einleitung 4
Projekthintergrund und Eckdaten des Projektes 4

Projektpartner **5**

Einführung digitale Transformation **6**

Einführung IT- und Cybersicherheit **7**

Analyse der öffentlichen Angriffsfläche **8**

Ergebnisse der Analyse der externen Angriffsfläche **12**
Debriefing – Versand individueller Berichte an die teilnehmenden Organisationen 14

Inhalte und Ablauf der Workshops **15**
Wortmeldungen aus den Workshops 16

Schlussfolgerungen **17**

Kontakt Autorinnen und Autoren **18**

Zum Projekt

Einleitung

Die digitale Transformation treibt strategische Veränderungen voran und setzt Potenziale frei. Gleichzeitig bringt sie auch Herausforderungen für Unternehmen mit sich, welche proaktiv adressiert werden sollten. Um diesen Veränderungen gerecht zu werden, sind Unternehmen (und Verwaltungen) gefordert, ihre Strategien und Geschäftsmodelle an den digitalen Bedürfnissen und Opportunitäten auszurichten und ihr Leistungsversprechen dem veränderten Markt anzupassen. Mit neuen oder adaptierten Geschäftsmodellen können Unternehmen einen Mehrwert für Kundinnen und Kunden schaffen und gleichzeitig die eigene Wettbewerbsfähigkeit stärken. Die IT- beziehungsweise Cybersicherheit ist dabei ein wichtiger Erfolgsfaktor für die Umsetzung von Unternehmensstrategien im digitalen Zeitalter.

Im Rahmen des europäischen Interreg-Projekts TITAN-E wurden gezielt kleine und mittelständische Unternehmen (KMU) in der Schweiz, in Süddeutschland und in Frankreich ausgewählt, um deren Website auf potenzielle Angriffsvektoren zu untersuchen. Am Ende der Analyse bekamen die 50 teilnehmenden Unternehmen die Möglichkeit, an einem von zwei Workshops, Ende Juni oder Anfang Juli 2023, Massnahmen zur Prävention von Angriffen mit einem Expertenteam des Cybersicherheits-Unternehmens Dreamlab Technologies zu diskutieren und individuelle Fragen hinsichtlich ihrer Berichte oder aktuellen Cybersicherheits-Lage in ihrem Unternehmen zu klären.

Projekthintergrund und Eckdaten des Projektes

Das Projekt wurde im Zeitraum Ende 2022 bis Juli 2023 mit den Projektpartnern Hochschule für Wirtschaft FHNW, Basel Area & Innovation und Dreamlab Technologies sowie mit 50 teilnehmenden Unternehmen in der Oberrheinregion (Fokus Nordwestschweiz, Elsass und Baden-Württemberg) durchgeführt. Die Unternehmen erklärten sich bereit, ihre Internet-Adressen (Domäne und IP-Adressen) im Rahmen einer Schwachstellenanalyse scannen zu lassen, um die öffentliche Angriffsfläche zu analysieren und so Einblick in ihre aktuelle digitale Bedrohungslage zu erhalten.

Die Resultate wurden den Unternehmen in individuellen Berichten zur Verfügung gestellt, und zwar im Vorfeld ihrer Teilnahme an den Online-Workshops. Den Abschluss des Projektes bildeten die zwei Workshops Ende Juni sowie Anfang Juli 2023. In diesen beiden Workshops wurden den Teilnehmenden, neben den anonymisierten Ergebnissen aus der Analyse, Inhalte zu den Themen digitale Transformation und IT-Sicherheit sowie Empfehlungen für die unternehmensinterne Cybersicherheit an die Hand gegeben. Die lebendigen Diskussionen der Teilnehmenden während der Online-Workshops sowie das Feedback zu den Workshops war durchwegs positiv und wertschätzend. Mit diesen positiven Rückmeldungen sowie der Publikation des vorliegenden Whitepapers wurde das Projekt TITAN-E der Hochschule für Wirtschaft FHNW in Olten erfolgreich abgeschlossen.

Projektpartner

Die Interviews wurden im Rahmen des Interreg-Projekts TITAN-E durchgeführt.

Zum Interreg-Projekt TITAN-E:
Das Projekt hat zum Ziel, das Potenzial des grenzüberschreitenden Ökosystems in der Oberrheinregion (Elsass, Baden-Württemberg, Schweiz) auszuschöpfen, indem Akteure aus Wissenschaft und Wirtschaft zusammengebracht und zu grenzüberschreitenden Projekten angeregt werden. Damit soll eine Zunahme der Entwicklung tri- oder binationaler Wirtschafts- und Geschäftsmodelle sowie Unternehmenskooperationen zwischen KMU gefördert werden.

Projektpartner:

Fachhochschule Nordwestschweiz / Hochschule für Wirtschaft
ist eine AACSB akkreditierte Hochschule, die mit ihrem Bildungsauftrag zu einem verantwortungsbewussten und innovativen Handeln in einer dynamischen Welt beiträgt.

Dreamlab Technologies
ist ein auf IT-Sicherheit spezialisiertes, internationales Beratungsunternehmen, das Unternehmen, Regierungen und die Verwaltung in den Bereichen IT- und Cybersicherheit unterstützt und Lösungskonzepte für eine sichere digitale Zukunft entwickelt.

Basel Area Business & Innovation
ist eine Non-Profit-Agentur, die Unternehmen, Institutionen und Start-ups bei der Vernetzung unterstützt und den Ausbau eines erfolgreichen Ökosystems in der Region Basel fördert.

Die Workshop-Reihe ist Teil des Interreg-Projekts TITAN-E und wird durch Bund und Kantone finanziell unterstützt.

Einführung digitale Transformation

Die Diskussionen in den beiden Online-Workshops im Juni und Juli 2023 bauten auf den Erkenntnissen der Workshop-Serie 2021 und der Best-Practice-Fallstudien 2022/2023 im Bereich digitale Transformation und IT-Sicherheit auf (www.trinational-digital-business.net). Für ein einheitliches Verständnis erscheint es sinnvoll, zunächst auf die relevanten Begriffe einzugehen (vgl. Peter, 2023).

Die Digitalisierung bezeichnet einen technischen Prozess, bei dem analoge Daten oder Abläufe in digitale umgewandelt beziehungsweise automatisiert werden. Viele Unternehmen versuchen papierlos zu arbeiten, Dokumente zu digitalisieren, sich über Kommunikationsplattformen auszutauschen sowie Arbeits- und Produktionsprozesse zu automatisieren. Doch ein Zugang zu einer Cloud und ein Benutzerkonto für Microsoft Teams bringen noch keine Transformation. Es handelt sich dabei lediglich um eine digitale Abbildung analoger Geschäftsabläufe. Im besten Fall werden dadurch Produktionskosten reduziert sowie die Qualität und Geschwindigkeit erhöht.

Die digitale Transformation beschreibt vielmehr eine Weiterentwicklung hin zu gegenwärtigen und künftigen Standards: Sie betrifft sowohl die Wirtschaft, das heisst die verschiedenen Funktionen innerhalb von Unternehmen und deren Geschäftsmodelle, als auch die Gesellschaft. Will – oder muss – sich ein Unternehmen digital transformieren, sollte sich die Geschäftsleitung also nicht in erster Linie fragen, wie sie bestehende Prozesse digitalisieren kann, sondern was das Unternehmen im digitalen Zeitalter strategisch machen muss, um weiterhin wettbewerbsfähig zu sein. Erst dann stellt sich die Frage der Digitalisierung und ob ein Prozess in der aktuellen Form überhaupt sinnvoll ist.

Im Kern der digitalen Transformation steht ein Praxismodell mit sieben Handlungsfeldern der digitalen Transformation. Diese bieten eine Orientierungshilfe für die Strategieentwicklung im digitalen Zeitalter:

1. Konstante Kundenorientierung
Unternehmen legen einen starken Fokus auf Kundenorientierung, personalisierte Angebote sowie digitale Kommunikations- und Absatzkanäle.

2. Neue Technologien
Die neuen Technologien beinhalten Plattformen und Apps. Viele Unternehmen testen die Anbindung an Industrie- und Konsumentenprodukte als Bestandteil der Industrie 4.0 beziehungsweise des Internet of Things.

3. Daten und die Cloud
Alle bisher genannten Aktivitäten bedürfen flexibler und von überall her zugänglicher Daten und Infrastrukturen. Bei den Daten geht es primär um das operative Daten-Management und die Datenqualität sowie die strategische Nutzung von Daten.

4. Neue Strategien und Geschäftsmodelle
Die neuen Technologien treiben Firmen dazu an, bestehende Angebote zu hinterfragen, um neue oder erweiterte Leistungen zu erbringen. Hier werden neue Plattformen genutzt sowie strategische Partnerschaften eingegangen, um innovative Geschäftsmodelle zu entwickeln.

5. Prozess-Management
Prozesse sollten standardisierter, schneller und effizienter gestaltet werden. Durch die Automatisierung beziehungsweise Digitalisierung der Prozesse können Teilaufgaben ohne Medienbrüche vernetzt werden.

6. Moderne Arbeitswelt
Durch den digitalen Wandel wird ein Veränderungsprozess ausgelöst, der zu einer Anpassung der Führungsgrundsätze führt. Zur modernen Arbeitswelt gehören Kreativität und Innovation, der digitale und mobile Arbeitsplatz sowie neue Organisationsformen.

7. Digitales Marketing
Durch die Verfügbarkeit und Analyse von Kunden-, Produkte- und Absatzdaten wird ein System geschaffen, in dem die Aktivitäten von Verkauf und Marketing laufend optimiert werden können. Dazu gehören Online-Plattformen, E-Commerce, Social Media, Suchmaschinen-Marketing und die Marketing-Automatisierung.

Abhängig von der Energie, Opportunität, Risikobereitschaft und Notwendigkeit werden die Potenziale digitaler Technologien und die Handlungsfelder der digitalen Transformation unterschiedlich priorisiert, behandelt und in der Strategie verankert.

Quelle:

Marc K. Peter
Digitaler Masterplan für KMU

So gelingt die digitale Transformation in Ihrem Unternehmen

1. Auflage 2023, 232 Seiten
ISBN 978-3-03875-458-9
www.digitaler-masterplan.ch

Einführung IT- und Cybersicherheit

Mit der digitalen Transformation gewinnt die IT-Sicherheit immer mehr an Bedeutung. Das damit verbundene komplexe und breite Themenspektrum fordert Unternehmen unterschiedlicher Grössen und geographischer Ausrichtung auf, sich darüber bewusst zu werden, wie und wie intensiv sie sich mit den unterschiedlichen Aspekten der IT-Sicherheit auseinandersetzen sollen.

Neben der physischen Sicherheit, die sich hauptsächlich auf die Sicherung von physischen IT-Infrastrukturen bezieht, geht es bei der Cybersicherheit um die Sicherung der Cyberdimension inklusive Netzwerke, Zugangsberechtigungen und Sensibilisierung der Mitarbeitenden im Unternehmen. Die Sicherung der nicht geschützten Netzwerke und Geräte wurde in den Online-Workshops mit einem Haus mit offenen Türen und Fenstern verglichen, das es einer potenziellen Angreiferin oder einem potenziellen Angreifer einfach macht, sich Zutritt zu den IT- und Datenkronjuwelen zu verschaffen. Aus diesem Grund ist es essenziell, sich zunächst ein Bild darüber zu verschaffen, welche Systeme oder Unternehmens-Assets von Angreifenden attackiert oder gar mithilfe einer Ransomware-Attacke stillgelegt werden könnten. Ein weiteres nicht zu unterschätzendes Risiko stellt das Thema «Social Engineering» dar. Heutzutage eher noch unterschätzt, gewinnt es insbesondere in den sozialen Medien immer mehr an Bedeutung. Unter «Social Engineering» wird die Technik der Manipulation verstanden, die das menschliche Verhalten ausnützt, um Zugriff zu Informationen, Daten oder Systemen zu erhalten.

Den genannten Risiken kann jedoch mithilfe gezielter Cybersicherheits-Massnahmen begegnet werden. Zu diesen Massnahmen gehören unter anderem folgende:

- Implementierung von Virtual Private Networks (VPNs) für einen sicheren Zugriff auf das Unternehmensnetzwerk
- Einsatz von starken Passwörtern
- Nutzung einer Multi-Faktor-Authentifizierung (2FA) (beispielsweise für E-Mail-Konten oder das Unternehmensnetzwerk)
- E-Mail-Verschlüsselung (beispielsweise mittels Pretty Good Privacy, kurz PGP)
- Implementierung von Backups
- Installation und Aktualisierung von Firewalls
- Sensibilisierung der Mitarbeitenden hinsichtlich Datenhygiene, Datenverschlüsselung und Angriffsmethoden

Aufgrund der aktuellen Nachrichtenlage wird Unternehmen zudem empfohlen, die eigene Netzwerk-Infrastruktur zu analysieren, um nicht Opfer einer Cyber-Attacke zu werden.

Ein ungeschütztes Computer-System ist ähnlich einem Haus mit offenen Türen und Fenstern (Quelle: N. Mayencourt & M. K. Peter, 2021).

Um Risiken zu minimieren, werden u. a. die folgenden Massnahmen empfohlen:

- Mitarbeitende hinsichtlich Phishing-Attacken sensibilisieren
- IT-Systeme kontinuierlich patchen und aktualisieren
- Netzwerke segmentieren, um die Gefahr einer flächenübergreifenden Infektion zu minimieren
- Multi-Faktor-Authentifikation (2FA) einführen
- regelmässige und verschlüsselte Offline- oder Cloud-Backups der Unternehmensdaten und -systeme erstellen
- regelmässig IT-Sicherheitsaudits sowie Sicherheitsübungen oder Ransomware-Simulationen durchführen

Diese Themen wurden in beiden durchgeführten Workshops besprochen.

Quelle:

Nicolas Mayencourt & Marc K. Peter
IT-Sicherheit für KMU

So navigieren Sie
Ihr Unternehmen sicher durch
Cyber-Turbulenzen

1. Auflage 2021, 176 Seiten
ISBN 978-3-03875-343-8
www.it-sicherheit-kmu.ch

Analyse der öffentlichen Angriffsfläche

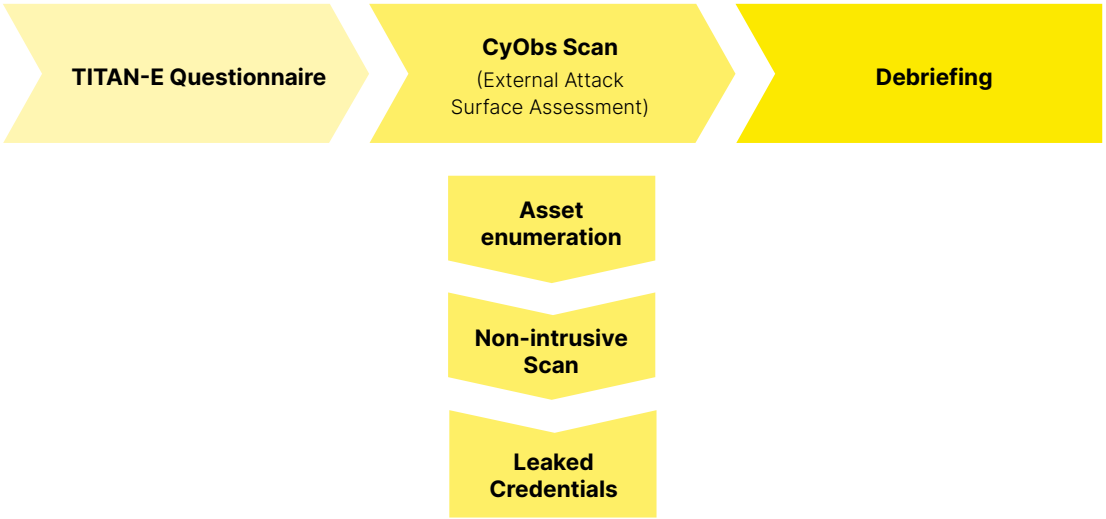
Im Folgenden soll die Vorgehensweise und angewandte Methodik zur Analyse der öffentlichen Angriffsfläche näher beleuchtet werden.

Basis der Untersuchung waren die Domänen und IPv4-Adressen der teilnehmenden Unternehmen. Diese wurden im Rahmen einer nicht-intrusiven Informationssammlungs-Kampagne mittels CyObs (www.cyobs.ch) anhand von öffentlich zugänglichen Quellen untersucht. Ohne tiefergehende Analyse liess sich allerdings nicht abschliessend klären, ob und wie die identifizierte Angriffsfläche für allfällige Angriffe tatsächlich ausgenutzt werden könnte.

CyObs ist die proprietäre Cyberradar-Lösung von Dreamlab Technologies zur Kartierung, Analyse und Visualisierung des Cyberspace eines Landes oder einer Organisation. Es identifiziert Cyberschwachstellen und die potenzielle Angriffsfläche noch vor einem potenziellen Angriff. CyObs ist der Startpunkt für die Entwicklung einer Cyberverteidigungsstrategie.

Im Zuge des Scans überprüfte Dreamlab Technologies die öffentlich zugängliche Internet-Infrastruktur der Unternehmen anhand der von ihnen zur Verfügung gestellten IP-Adressen und Domänennamen, um einen allgemeinen Eindruck über die öffentliche Angriffsfläche und somit die Sicherheit zu erhalten. Daneben wurden alle identifizierten Domänen auf mögliche Einträge in Darknet-Passwortdatenbanken überprüft. Bei dieser Vorgehensweise wurden keinerlei Sicherheitsfunktionen der Systeme umgangen. Die durchgeführten Scans sind nicht mit einem IT-Sicherheitsaudit gleichzusetzen und ersetzen dieses nicht.

Nach der Analyse wurden die Daten in individuellen Berichten für die teilnehmenden Firmen aufgearbeitet und diesen im Vorfeld der Workshops zugestellt. In den Workshops selbst wurde auf die kumulierten Analyseergebnisse aller Unternehmen anonymisiert eingegangen, das heisst ohne Nennung von individuellen Resultaten.



Studienvorgang IT-Sicherheitsanalyse im Rahmen des TITAN-E-Projektes

Schritt 1: Aufzählung der IT-Infrastrukturkomponenten («Asset Enumeration»)
Die Aufzählung von IT-Infrastrukturkomponenten (IT-Assets) ist ein entscheidender Teil jeder Bewertung der externen Angriffsfläche einer Organisation und gehört in der einen oder anderen Form auch zu fast jedem echten Cyberangriff.

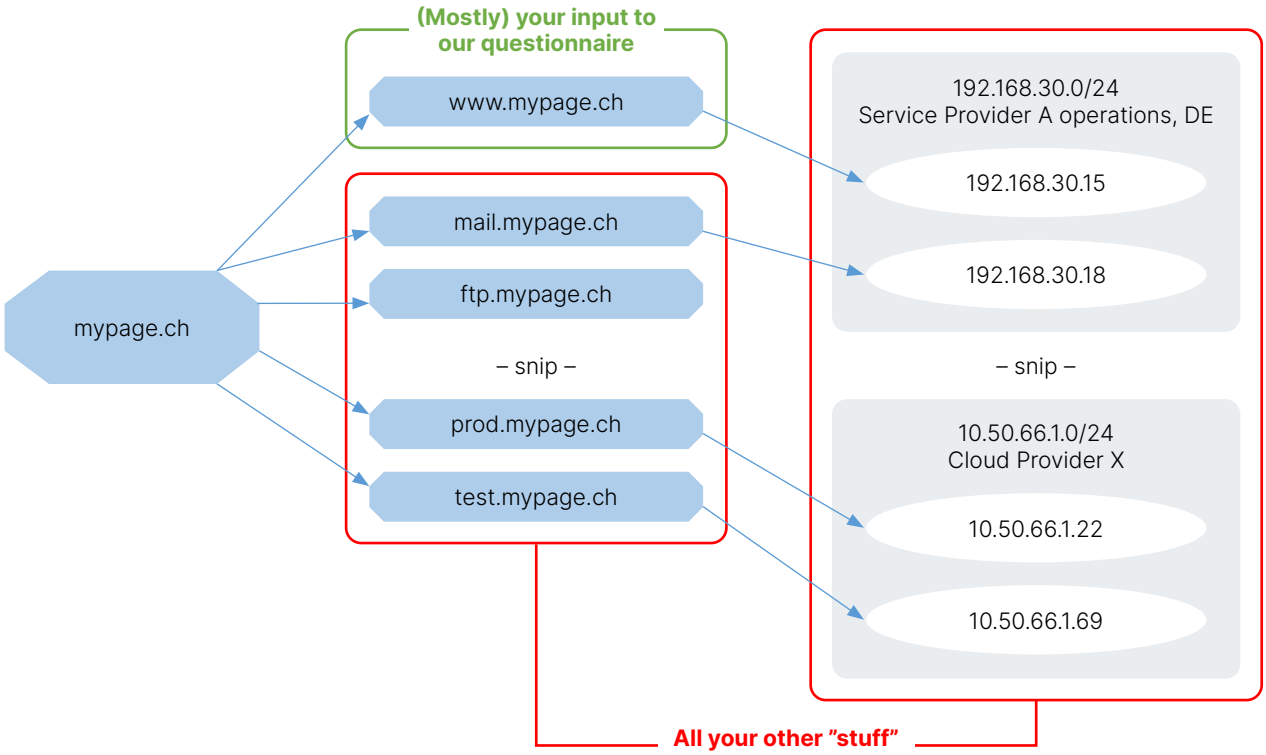
Ziel der «Asset Enumeration» ist es, eine Liste der mit einer Organisation zusammenhängenden Domänen, Subdomänen und IP-Adressen bzw. Server und Services zu erstellen. Die Gesamtheit der so identifizierten Infrastruktur stellt die externe Angriffsfläche einer Organisation dar. Die nachfolgenden Abschnitte zeigen dies am Beispiel der fiktiven Domäne «mypage.ch».

In diesem Schritt wurde die Asset Enumeration mit einer bestimmten Domäne wie zum Beispiel «mypage.ch» basierend auf den Eingaben der Teilnehmehmenden begonnen. In diesem Beispiel könnte es sich um www.mypage.ch handeln, das auf die Website der Organisation verweist.

In der Regel veröffentlicht eine Organisation im Internet mehr Dienste als nur die Website, welche z.B. via www.mypage.ch erreichbar ist. Die Informationen, wie diese zusätzlichen Dienste zu finden sind (die sogenannten Subdomänen wie beispielsweise «ftp.mypage.ch» oder «mail.mypage.ch» sowie zusätzliche Domänen wie «adifferentname.ch»), können von allen Personen (auch von potenziellen Angreifenden) frei und einfach beschafft werden.

Sobald die verfügbaren Domänen und Subdomänen für eine Organisation aufgelistet («enumeriert») sind, werden diese Elemente in eine numerische Darstellung, die sogenannte IP-Adresse, aufgelöst. Jede identifizierte IP-Adresse identifiziert eindeutig einen Server, der mit dem Internet verbunden ist und irgendeinen Zweck für die betreffende Organisation erfüllt.

Jeder Dienst und jeder Server, der von einer Organisation veröffentlicht wird, ist potenziell angreifbar und stellt somit ein Risiko für die Organisation dar. Die folgende Abbildung veranschaulicht die Beziehung zwischen Domäne, Subdomänen und IP-Adressen (von links nach rechts).

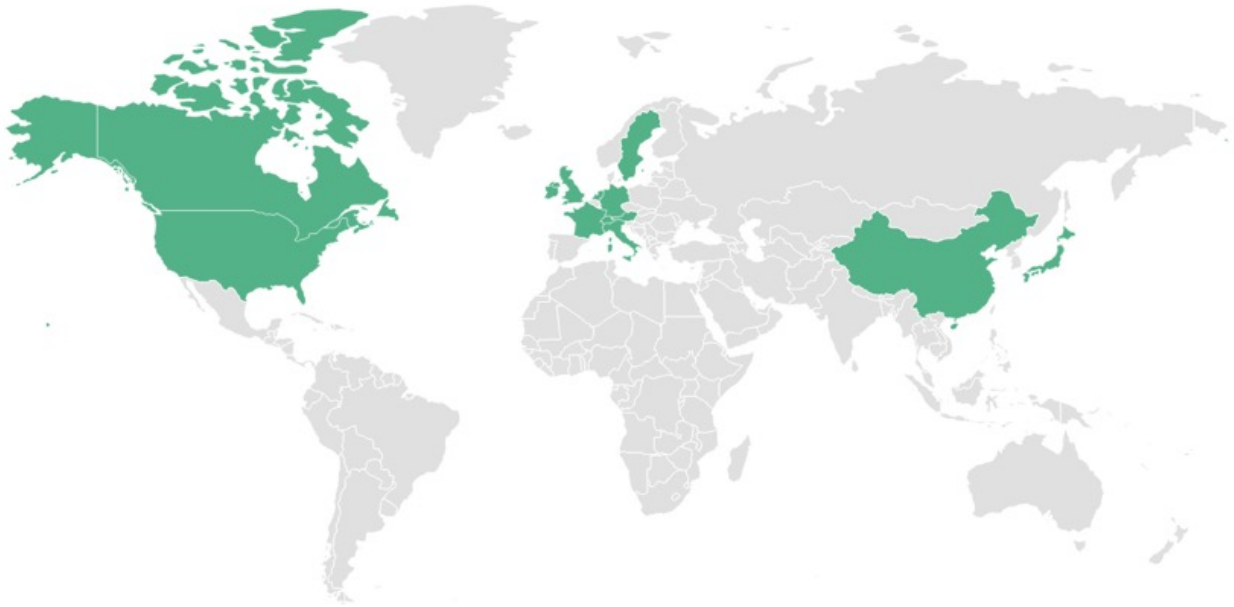


Beziehung zwischen Domäne, Subdomänen und IP-Adressen (von links nach rechts)

Es ist wichtig zu verstehen, dass die IT-Infrastruktur einer Organisation in der Regel viel mehr umfasst, als auf den ersten Blick, zum Beispiel mittels Besuch auf der Website, ersichtlich ist.

Dies gilt auch aus geografischer Sicht. Sobald die IP-Adressen im Zusammenhang mit der IT-Infrastruktur einer Organisation bekannt sind, können sie geografisch lokalisiert werden. Es stellt sich also bereits die Frage, ob sich die teilnehmenden Firmen aus der Oberrheinregion bewusst waren (siehe Abbildung), dass ihre IT-Infrastrukturen in dieser Breite global verteilt sind.

Die Geolokalisierung der IP-Adressen (der Server) aller fünfzig TITAN-E-Teilnehmenden ergibt das folgende Resultat auf der abgebildeten Weltkarte.



Geolokalisierung der IP-Adressen der 50 teilnehmenden Organisationen (CyObs)

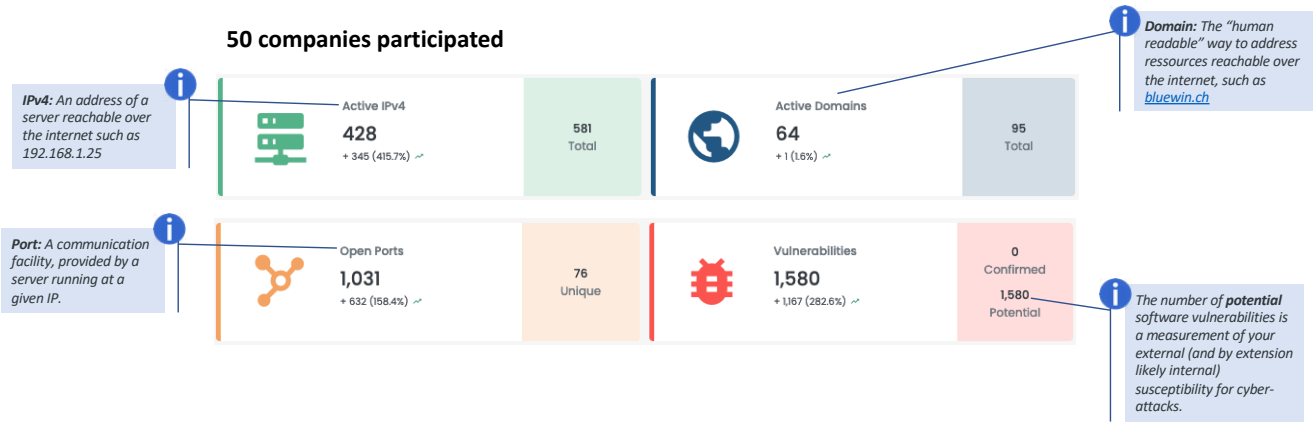
Schritt 2: Nicht-intrusiver Scan
Sobald die Liste der relevanten Domänen, Subdomänen und IP-Adressen bekannt ist, wird diese automatisch von CyObs überprüft. Dazu führt CyObs einen sogenannten «Port Scan» durch, um verfügbare Dienste zu identifizieren (Ein Port ist ein Kommunikationsmechanismus, der von einem Server unter einer bestimmten IP bereitgestellt wird.). Die identifizierten Dienste werden im Anschluss von CyObs aufgesucht und analysiert. In der Regel veröffentlicht ein Web-Dienst Informationen darüber, welche Software er genau ausführt (das sogenannte «Dienstbanner»). So können Marke, Modell und Version der Software identifiziert werden, die für die Bereitstellung des Dienstes verwendet werden. Dies sind wertvolle Informationen, da sie CyObs erlauben, einen Abgleich mit (ebenfalls öffentlich und frei zugänglichen) Datenbanken bekannter Software-Schwachstellen durchzuführen.

Diese relevanten Informationen ermöglichen CyObs, potenziell vorhandene Software-Schwachstellen zu identifizieren. Eine potenzielle Schwachstelle bedeutet nicht, dass ein bestimmter Dienst von einer Schwachstelle betroffen ist, sondern nur, dass er es sein könnte. Die Anzahl der potenziellen Schwachstellen ist jedoch ein erster Anhaltspunkt dafür, wie gut ein bestimmter Server gewartet wird und wie hoch das Risiko für das Unternehmen ist.

Schritt 3: Prüfung auf durchgesickerte (gestohlene und publizierte) Zugangsdaten
Ein weiterer wichtiger Aspekt in Bezug auf die externe Angriffsfläche einer Organisation sind gestohlene beziehungsweise durchgesickerte, das heisst publizierte, Anmeldedaten (wie Benutzernamen und zugehörige Passwörter). Teilweise nutzen Benutzerinnen und Benutzer in Organisationen ihre beruflichen Identitäten für Drittanbieterdienste wie Facebook oder LinkedIn. Manchmal werden diese Drittanbieterdienste selbst gehackt und die Benutzerinformationen, einschliesslich der Benutzernamen und Passwörter, gestohlen. Es ist dann möglich, dass die Angreiferinnen und Angreifer diese gestohlenen Anmeldedaten wiederverwenden und versuchen, sich bei den Diensten eines Unternehmens anzumelden, um sich einen ersten Zugang zu verschaffen. Aus diesem Grund werden Anmeldedaten, die mit identifizierten Domänen übereinstimmen (während der Aufzählung der IT-Infrastrukturkomponenten), in die Analyse der externen Angriffsfläche einer Organisation einbezogen.

Ergebnisse der Analyse der externen Angriffsfläche

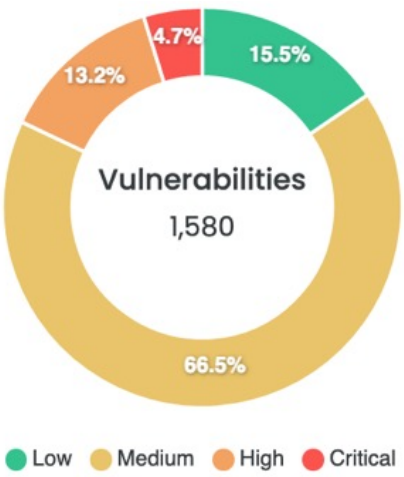
Die Analyse der externen Angriffsfläche hat in Bezug auf alle 50 Studienteilnehmenden Folgendes ergeben:



Übersicht der Analyseergebnisse der 50 teilnehmenden Organisationen (CyObs)

Es gab etwa neunmal so viele IP-Adressen (428) wie teilnehmende Unternehmen. Einige Organisationen verwendeten mehr als eine Domäne. Insgesamt zählen die Unternehmen 64 Domänen. Die 50 teilnehmenden Organisationen betreiben insgesamt 1 031 Dienste in ihrer Infrastruktur, die 1 580 potenzielle Sicherheitslücken aufweisen.

Werden die Schwachstellen mit Hilfe des Common-Vulnerability-Scoring-Systems (CVSS) nach ihrer Kritikalität eingestuft, ergibt sich folgende Statistik:



Übersicht der Schwachstellen der 50 teilnehmenden Organisationen nach Kritikalität (CyObs)

Die Studie ergab, dass die Zugangsdaten bei etwa der Hälfte der teilnehmenden Unternehmen von mindestens einem oder zwei Nutzenden (in einem Extremfall von bis zu 252 Nutzenden) durchgesickert sein könnten.

Neben den oben genannten Ergebnissen wurden in der Studie auch eine Reihe von Datenbank-Servern identifiziert, die mit dem offenen Internet verbunden sind. Dies bedeutet, dass die Datenbank-Server verfügbar sind, aber nicht unbedingt, dass Daten aus diesen Datenbanken zugänglich sind.

Name der Software	Anzahl
MySQL 5.7.41	7
MySQL 4.96	4
MariaDB 10.6.13	4
MariaDB 10.6.12	3
MySQL 5.7.42	3
Mysql 5.5.5-10.6.13-mariadb	3
Mysql 5.5.5-10.6.12-mariadb	3
Postgresql db 9.6.0 oder früher	2
Mysql 5.7.42-0ubuntu0.18.04.1	2
Mysql 3.23.57	1
MariaDB 10.4.30	1
MariaDB 5.5.68	1
MariaDB 10.4.28	1
Mysql 5.5.5-10.3.38-mariadb	1
MySQL 3.23.57	1
Mysql 5.5.68-mariadb	1
Mysql 5.5.5-10.4.30-mariadb	1
MariaDB 10.5.19	1
Mysql 5.5.5-10.4.28-mariadb	1
MariaDB 10.3.38	1
MariaDB 10.5.21	1

Übersicht der öffentlich zugänglichen Datenbank-Server der 50 teilnehmenden Organisationen (CyObs)

Zudem wurde eine Reihe von FTP-Servern identifiziert. FTP steht für «File Transfer Protocol» (Dateiübertragungsprotokoll) und ist eine gängige Technik für den Datenaustausch, zum Beispiel mit Web-Servern, und wird häufig als «behelfsmässige» Plattformlösung für den Datenaustausch mit Partnerfirmen und der Kundschaft verwendet.

Softwarename	Anzahl
ProFTPD	12
PureFTPd	12
Proftpd mod_sftp 0.9.9	1
ProFTPD 1.3.5e	1

Übersicht der öffentlich zugänglichen FTP-Server der 50 teilnehmenden Organisationen (CyObs)

Die Datenbanken und FTP-Server sind ein leichtes Ziel zum Verproben der geleakten Credentials und um zu sehen, ob ein Login möglich ist.

Die Studie identifizierte darüber hinaus mindestens zwei sensible Dienste, die im Internet veröffentlicht wurden. Aufgedeckt wurden eine Gitlab-Instanz (ein «Quellcode-Repository»), die historisch mehrmals von Sicherheitslücken betroffen war, sowie eine Grafana-Instanz (eine Datenanalyse- und Visualisierungsplattform), welche in der identifizierten Version des teilnehmenden Unternehmens angegriffen werden könnte.

Debriefing – Versand individueller Berichte an die teilnehmenden Organisationen

Aus der Studie und den daraus resultierenden Berichten lassen sich folgende Handlungsempfehlungen für die teilnehmenden Organisationen ableiten:

Zuerst sollten die verschiedenen Dienstleistungen, die eine Organisation in Anspruch nimmt, der Reihe nach überprüft werden. Für jeden Dienst gilt es, die folgende Frage zu klären:

- Muss dieser Dienst über das offene Internet zugänglich sein? (Datenbanken, FTP, Grafana, Gitlab, ...)
- Wenn nein: Der Dienst sollte entfernt werden oder hinter einer Firewall beziehungsweise einem VPN versteckt werden.
- Wenn ja: Der Dienst sollte regelmässig gepatcht und aktualisiert werden und sein Dienstbanner sollte, wenn möglich, versteckt werden.

Zweitens sollten die durchgesickerten (gestohlenen und publizierten) Anmeldedaten überprüft und die Passwörter der betroffenen Benutzerinnen und Benutzer geändert werden. Es ist wichtig, alle betroffenen Systeme zu berücksichtigen. Da einige kleinere Organisationen keine zentrale Benutzerverwaltung haben, kann dies bedeuten, dass jeder Dienst einzeln überprüft werden muss.

Inhalte und Ablauf der Workshops

Im Rahmen der Workshops lag der Schwerpunkt auf den beiden Themen digitale Transformation und IT-Sicherheit beziehungsweise Cybersicherheit. Im ersten der beiden zweistündigen Workshops, am 21. Juni 2023, nahmen 26 Unternehmen teil. Am 5. Juli 2023 waren es zehn Unternehmen (gesamthaft partizipierten 36 der 50 teilnehmenden Organisationen). Die Workshops wurden in Englisch durchgeführt.

Die Themen der Workshops:

Thema	Referierende/r	Zeit
Digitale Transformation – Einleitung	Anna V. Rozumowski / Marc K. Peter	10 min.
Cybersicherheit – Einleitung	Konstanze Schäfer	10 min.
Q&A, Diskussion	Alle Teilnehmenden	10 min.
Cybersicherheit für KMU	Jacek Jonczy	20 min.
Q&A, Diskussion	Alle Teilnehmenden	10 min.
Coffee Break		10 min.
CyObs: Resultate der teilnehmenden SMEs	Mischa Obrecht	20 min.
Q&A, Diskussion	Alle Teilnehmenden	10 min.
Wrap-up, nächste Schritte	Konstanze Schäfer	10 min.

Agenda der Workshops vom 21. Juni und 5. Juli 2023

Nach jedem Themenabschnitt wurde den Teilnehmenden die Möglichkeit eingeräumt, Fragen zu den jeweiligen Inhalten zu stellen. Diese Möglichkeit wurde in beiden Workshops rege genutzt.

Nach der kurzen Einführung ins Thema digitale Transformation wurde im Einführungsbeitrag zur Cybersicherheit eine Einleitung zu den grössten IT-Sicherheitsproblemen beziehungsweise wichtigsten Massnahmen zur Erhöhung der Cybersicherheit präsentiert.

Nach einer ersten interaktiven Runde mit den Teilnehmenden wurden die technischen Aspekte der IT-Sicherheit bei KMU präsentiert. Dabei stellte sich heraus, dass KMU sehr unterschiedlich mit dem Thema Cybersicherheit umgehen. Je nach Grösse und technischem Know-how hatten sich bereits einige der technischen Massnahmen wie Firewalls, eine Segmentierung der unterschiedlichen Netzwerke oder eine Multi-Faktor-Authentifizierung (2FA) etabliert. Unter den teilnehmenden KMU befanden sich auch Unternehmen, die ihre IT-Sicherheit an externe IT-Dienstleister auslagerten. In dieser Geschäftsbeziehung wurden dann sogenannte Service-Level-Agreements (SLA) getroffen, welche die Leistungen definieren. Unter dem letzten Agendapunkt wurden die Analyseergebnisse des CyObs-Scans präsentiert. Dieser Überblick ermöglicht den 36 an den Workshops teilnehmenden Unternehmen, ihre individuellen Ergebnisse in einen Kontext zu setzen.

Wortmeldungen aus den Workshops

Die folgenden Wortmeldungen wurden notiert:

Themenblock 1: Einführung in die Themenbereiche

Verfolgen Sie eine Strategie hinsichtlich des Themengebietes der digitalen Transformation in Ihrem Unternehmen?

Stimmen der Teilnehmenden:
- «Wir haben zwar keine Strategie im Bereich digitale Transformation, aber wir nutzen digitale Tools.»
- «Digitale Transformation: nicht wirklich eine Strategie.»
- «Keine Ahnung.»
- «Wir sind gerade dabei, einen Teil [davon] zu definieren.»
- «Wir wissen, dass wir da etwas machen müssen, aber die Prioritäten liegen aktuell woanders.»
- «Hinsichtlich der digitalen Transformation machen wir etwas, und es beginnt mit Projekten und Zeitplänen.»
- «Es gibt einige Projekte, aber ich bin mir der Strategie nicht bewusst.»

Haben Sie eine Cybersicherheits-Strategie in Ihrem Unternehmen?

Stimmen der Teilnehmenden:
- «Wir haben zwar eine Cybersicherheits-Strategie, aber keine für die digitale Transformation. Wir sind unsicher, wohin uns die Zukunft führen wird. Wir dachten, wir seien auf einem guten Weg, doch jetzt sind wir ein wenig verloren.»
- «Wir haben Ideen und arbeiten parallel an unterschiedlichen Themen. Aber ich würde das als keine Strategie (…) beschreiben.»
- «Cybersicherheit wird [bei uns] durch erzwungene Regulierungen definiert.»
- «Zusammen mit unserem IT-Manager haben wir eine Strategie definiert.»
- «Als kleines Unternehmen versuchen wir, die notwendigsten Massnahmen zu ergreifen: Wir legen fest, wer wie Zutritt hat, trennen Bereiche für Gäste und interne Mitarbeitenden (…) mit einem Passwort-Manager (…). Wir arbeiten an weiteren Verbesserungen – es ist eine permanente Baustelle.»
- «Wir arbeiten aktuell an einem Onboarding-Prozess, damit Cybersicherheit und digitale Transformation im Start-Paket mitaufgenommen sind und die neuen Mitarbeiter auf die Themen sensibilisiert werden.»
- «Wir lagern die Sicherheitsmassnahmen an IT-Partner wie Microsoft aus. Die Sicherheitsprobleme müssen sich erst einspielen, wenn man nicht über das entsprechende Know-how im Unternehmen verfügt, sonst macht man es falsch. Wir überlassen diese Fragen unseren Partnern, die Anwendungen hosten, und stellen sicher, dass sie alle Sicherheitsmassnahmen ergreifen, um einen sicheren Betrieb zu gewährleisten.»

Themenblock 2 und 3: IT-Sicherheit bei KMU

Waren Sie schon einmal von einem Cyberangriff betroffen? Wenn ja, welche Erfahrungen haben Sie gemacht und welche Konsequenzen haben Sie daraus gezogen?

Stimmen der Teilnehmenden:
- «Die Führungsebene hat die IT-Sicherheit nicht verstanden oder ist sich des Risikomanagements nicht bewusst, nach dem Motto: Wir sind nicht hackbar.»
- «Das Management hat oft das Gefühl, dass alles sicher ist und schätzt die IT-Sicherheit nicht. Sprechen Sie über Angriffe und was Sie verhindert haben! Kommunikation ist der Schlüssel! Es geht nicht nur darum, für die IT-Sicherheit zu bezahlen, sondern auch darum, zu erklären, dass zum Beispiel nichts passiert ist.»
- «Wir haben einen Online-Shop («Open Source») verwendet, der über Nacht einen Patch aufgespielt hat. Und dieser Patch enthielt Malware, die in unsere Produktivsysteme eingeschleust wurde. Es war sichtbar, da wir eine Überwachung hatten. Tipp: Überwachen Sie Ihren Dienst. Wenn etwas Seltsames passiert: Seien Sie wachsam – 24/7.»

Haben Sie Tipps, wie man das Thema Cybersicherheit angehen könnte?

Stimmen der Teilnehmenden:
- «Bestandsaufnahme der IT-Assets – was man nicht kennt, kann man auch nicht kontrollieren. Es ist besser, sich einen guten Überblick über den Bestand des Unternehmens zu verschaffen, dann kann eine Analyse der potenziellen Schwachstellen vorgenommen werden.»

Schlussfolgerungen

Das TITAN-E-Teilprojekt zur «Analyse und Sensibilisierung IT-Sicherheit» hat gezeigt, dass KMU in den Bereichen digitale Transformation und IT-Sicherheit noch viel Potenzial und Handlungsbedarf haben.

Vielen Unternehmen fehlt es nach wie vor am Wissen, wie sie die beiden Themen am effizientesten «anpacken» können. Das ist in den Gesprächen mit den unterschiedlichen Unternehmen deutlich geworden. Insbesondere in den oberen Führungsetagen liegt auf diesen beiden Themen-Komplexen noch das Stigma der Unsicherheit. Solange diesen beiden Themen nicht der notwendige Stellenwert eingeräumt wird, wird es Unternehmen schwerfallen, sie im digitalen Zeitalter in ihre Unternehmensstrategie zu integrieren.

Die Relevanz der digitalen Transformation, und damit einhergehend der IT-Sicherheit, ist ungebrochen und wird in den kommenden Jahren stetig zunehmen, insbesondere getrieben durch neue Themenfelder wie Blockchain, künstliche Intelligenz und das Web 3.0 (Stichwort Metaverse). Diesen Entwicklungen können sich Unternehmen unterschiedlicher Branchen und Grössen nicht verschliessen. Aus diesem Grund empfiehlt es sich, sukzessiv digitale Themen in relevanten strategischen Diskussionen auf der Ebene der Entscheiderinnen und Entscheider zu adressieren sowie sie anhand ihrer möglichen Adaption auf das Tagesgeschäft zu evaluieren und zu priorisieren. Damit einhergehend sollten auch Massnahmen möglicher IT-Risiken besprochen werden, um die Unternehmen zukunftsfähig und resistenter gegen Risken aufzustellen.

Mit einem holistischen und langfristigen Blick auf den Schutz der digitalen Kronjuwelen haben Unternehmen die Möglichkeit, sich den Themen der Zukunft gegenüber gestärkt und offen zu präsentieren. Die digitale Transformation präsentiert und konfrontiert Unternehmen mit den strategischen Potenzialen im digitalen Zeitalter: Die IT-Sicherheit ist der Erfolgsfaktor für die erfolgreiche Umsetzung einer digitalen Strategie.

Wundervolle Initiative.
Vielen Dank im Namen aller SMEs.

(Feedback Workshop-Teilnehmer/in)

Vielen Dank für das interessante Meeting und die Präsentationen.

(Feedback Workshop-Teilnehmer/in)

Wir haben besser verstanden, wo wir etwa stehen, wo wir gut aufgestellt sind und in welchen Bereichen wir Verbesserungen prüfen müssen.

(Feedback Workshop-Teilnehmer/in)

Danke für die Unterlagen. Das Webinar war aufschlussreich und hat uns weitere Informationen geliefert.

(Feedback Workshop-Teilnehmer/in)

Kontakt Autorinnen und Autoren

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

Anna V. Rozumowski
Hochschule für Wirtschaft FHNW
anna.rozumowski@fhnw.ch

Konstanze Schäfer
Dreamlab Technologies AG
konstanze.schaefer@dreamlab.net

Jacek Jonczy
Dreamlab Technologies AG
jacek.jonczy@dreamlab.net

Mischa Obrecht
Dreamlab Technologies AG
mischa.obrecht@dreamlab.net

Marc K. Peter, Konstanze Schäfer, Anna V. Rozumowski,
Jacek Jonczy und Mischa Obrecht:

Analyse und Sensibilisierung IT-Sicherheit
Workshops IT-Sicherheit und
Analyse der öffentlichen Angriffsfläche
TITAN-E Projet Européen

Olten, Juli 2023

Folgende Hochschulen der Fachhochschule
Nordwestschweiz FHNW bieten Weiterbildungen an:

– Hochschule für Angewandte Psychologie FHNW
– Hochschule für Architektur, Bau und Geomatik FHNW
– Hochschule für Gestaltung und Kunst Basel FHNW
– Hochschule für Life Sciences FHNW
– Hochschule für Musik Basel FHNW
– Pädagogische Hochschule FHNW
– Hochschule für Soziale Arbeit FHNW
– Hochschule für Technik FHNW
– Hochschule für Wirtschaft FHNW

Fachhochschule Nordwestschweiz FHNW
Hochschule für Wirtschaft
Riggenbachstrasse 16
CH-4600 Olten
info.wirtschaft@fhnw.ch

www.fhnw.ch/wirtschaft