IT-Security

Technologie Report

Wien,
Mai 2020

Sehr geehrte Leserinnen und Leser,

Wien zählt zu den Top 5 der IKT-Metropolen Europas. Rund 6.200 IKT-Unternehmen (8% der Unternehmen in Wien) erwirtschaften hier einen Umsatz von mehr als 20 Milliarden Euro jährlich. Die rund 8.900 landesweiten und internationalen IKT-Firmen in der „Vienna Region“ (Wien, Niederösterreich und Burgenland) sind für gut zwei Drittel des gesamten Umsatzes der IKT-Branche in Österreich verantwortlich.

Laut verschiedenen Studien punktet Wien besonders stark mit Innovationskraft, der umfassenden Unterstützung von Startups sowie einem starken Fokus auf Nachhaltigkeit. Auch in mehreren „Smart City“-Rankings liegt Wien auf den vordersten Plätzen. Der Standort überzeugt außerdem durch sein forschungs- und technologiefreundliches Klima, die geographische und kulturelle Nähe zu den Wachstumsmärkten im Osten, die hohe Qualität der Infrastruktur und des Ausbildungssystems sowie nicht zuletzt die weltweit höchste Lebensqualität.

Mit der Strategie „Wien 2030“ fokussiert die Bundeshauptstadt auf jene Themen, bei denen die Stadt bereits besonders erfogreich ist und will so Antworten auf die großen Herausforderungen der kommenden Jahre – vom Klimawandel bis zur Digitalisierung – geben. In diesen Bereichen will Wien in den nächsten zehn Jahren zur Weltspitze gehören und besonders kraftvolle Innovationen („Wiener Lösungen“) entwickeln. Eines der Wiener Spitzenthemen ist die „Wiener Digitalisierung“. Hier ist Cyber Security ein wesentlicher Schwerpunkt, der Aufbau eines Cyber Security Hubs wird als eines der Leitprojekte umgesetzt.[1]

Um das Potenzial an diesem Standort optimal zu nutzen, fungiert die Wirtschaftsagentur Wien als Informations- und Kooperationsplattform für Wiener Technologieentwicklerinnen und -entwickler. Sie vernetzt Unternehmen mit Entwicklungspartnerinnen und Leitkunden aus Wirtschaft, Wissenschaft und Stadtverwaltung und unterstützt die Wiener Unternehmen mit gezielten monetären Förderungen und einer Vielzahl von Beratungs- und Serviceangeboten.

Der vorliegende Technologie Report bietet daher einen Überblick über die verschiedensten Trends und Entwicklungen zu dem Thema „IT-Security in Wien“ insbesondere unter Berücksichtigung entsprechender Know-How-Trägerinnen und Akteure sowie von Aktivitäten in Wien.

Ihr Team der Wirtschaftsagentur Wien

1

Wien 2030 Wirtschaft & Innovationen,
https://stolzauf.wien.gv.at

EFRE Europäische Union Investitionen in Wachstum & Beschäftigung. Österreich
wirtschaftsagentur wien
Für die Stadt Wien

Inhalt

1. IT-Security – Von der Kür zur Pflicht

Informations- und Kommunikationstechnologien durchdringen heutzutage alle Lebensbereiche wie auch alle wichtigen Wirtschaftsbranchen – und die Zahl der Internetnutzer, der Smartphones sowie die Vielfalt der digitalen Angebote im Allgemeinen steigt kontinuierlich. Durch die Vernetzung von Milliarden Geräten („Internet of Things“) werden die Vorteile digitaler Technologien vervielfacht, allerdings nehmen damit auch die Möglichkeiten für Angriff und Missbrauch zu.

Ganz abgesehen von den üblichen digitalen „Schädlingen“ boomen Attacken auf Unternehmen und Industriespionage. Speziell durch die stärkere Nutzung von Handys und Tablets – auch aus eigenem Besitz („Bring Your Own Device“) – sehen sich Unternehmen mit neuen Risiken bezüglich IT-Sicherheit konfrontiert. Egal ob „Industrie 4.0“, Cloud-Computing oder klassische Bürolösung: Stabile Netze, eine verlässliche Infrastruktur und die klassische IT-Sicherheit sind laut Experten keine Kür mehr, sondern Pflicht.

Schon längst geht es nicht mehr nur um den Schutz einzelner PCs, sondern auch um die gesamte IT-Infrastruktur. Nicht erst der bereits eingetretene Notfall zwingt dazu, sich mit dem Thema zu beschäftigen. Informationstechnologie muss als Querschnittsmaterie inzwischen in allen Bereichen mitgedacht und geplant werden, somit hat IT-Security eine immer stärkere strategische Dimension, auch als Standortfaktor für die gesamte (Wiener) Wirtschaft.

2. Cyberbedrohungen sind allgegenwärtig

Über die Hälfte der Weltbevölkerung (2016: 44 Prozent) ist in der einen oder anderen Form mit dem Internet verbunden. Schon heute nutzen 510 Millionen Menschen – das sind über 90% – in Europa das Internet. Diese Vernetzung bietet viele Chancen, aber birgt auch viele Gefahren. Dies spiegelt sich zum Beispiel in dem 2017 erschienenen WEF Global Risk Report[2] wider, demzufolge die Wahrscheinlichkeit, Opfer einer Cyberattacke oder eines Datendiebstahl zu werden, zu den fünf größten Risiken weltweit zählt.

Mit jedem Jahr nimmt die Anzahl der Bedrohungen nicht nur zu, sondern auch die Bedrohungslandschaft an sich ist einem regen Wandel unterworfen. Während früher insbesondere DDoS-Angriffe beliebt waren, werden diese zunehmend durch APTs (Advance Persistant Threats) und Ransomware/Verschlüsselungstrojaner verdrängt. Letztere konnte laut dem österreichischen Bundeskriminalamt zwischen 2016 und 2017 mit mehr als 186% den größten Anstieg verzeichnen. Diese rasante Zunahme an Ransomware spiegelt sich auch in zahlreichen Vorfällen weltweit wider. Der brisanteste Vorfall bildet dabei ein Angriff auf den südkoreanischen Webhoster Nayana: Dieser zahlte eine Rekordsumme von 1,3 Milliarden Won (1,14 Millionen US-Dollar) an die Angreifer, um wieder an seine verschlüsselten Daten gelangen zu können.[3]

Durch die zunehmende Vernetzung von Gegenständen mit dem Internet (Internet of Things, kurz IoT) hat sich die Problematik von Cyberangriffen weiter signifikant verschärft. Mittlerweile weist jeder europäische Haushalt im Durchschnitt bereits 14 solcher IoT-Geräte auf. Die meisten von diesen sind für Cyberangreifer leicht angreifbar und weisen größtenteils schwache Passwörter auf, die teilweise nicht einmal abgeändert werden können. Dies erlaubt es Angreifenden sich relativ einfach Zugriff zu diesen Geräten zu verschaffen und sie zu steuern. Aufgrund der Vernetzung der Geräte miteinander kann dadurch ebenso leicht auf die Systeme anderer Geräte zugegriffen werden und in Folge sensible Daten ausgelesen werden. Viele Personen aber auch Unternehmen sind sich dieser Gefahr bisweilen zu wenig bewusst, dass beispielsweise aufgrund eines vorhandenen Smart-TV im Betrieb vertrauliche Daten von anderen Computern entwendet werden können, und ergreifen dementsprechend oftmals nur geringe oder überhaupt keine entsprechenden Präventionsmaßnahmen.

Der Einsatz von neuen Technologien wird die Unternehmen zukünftig ebenso vor zusätzliche Sicherheits-Anforderungen stellen. So geht zum Beispiel künstliche Intelligenz mit der Entwicklung neuer Bedrohungen einher. Ein internationales Forschungsteams unter Leitung des Max-Planck-Instituts für Informatik, Saarbrücken, präsentierte zu diesem Thema eine Arbeit zu einem Verfahren namens „Deep Video Portraits“ vor.[4] Dieses Verfahren erlaubt es, täuschend echte Videofälschungen zu erzeugen („deepfakes“). So könnten zum Beispiel Videos von politischen Gegnern oder anderen wichtigen Mitgliedern der Gesellschaft verwendet werden, um deren Reputation gezielt zu schädigen.

Ein weiterer neuer Faktor zeigt sich in der Verwendung von Cloud-Services. Immer mehr Unternehmen nutzen einen Cloud Service Provider (CSP) und lagern Elemente ihrer Datenspeicherung, Analyse und Informationstechnologie-Funktionen aus. Durch den Verlust von Cloudbasierten Lösungen kann der Geschäftsbetrieb schnell und umfangreich gestört sein. Einen kleinen Vorgeschmack gab die Betriebsstörung von Teilen des Cloud-Computing-Dienstes von Google am 17. Juli 2018, was den vorübergehenden Ausfall einiger populärer Anwendungen nach sich zog, einschließlich Snapchat, Spotify and Discord. Auch ein Sturm nahe eines in Texas liegenden Cloud-Rechenzentrums sorgte am 4. September 2018 für den Ausfall eines Großteils von Microsoft Azure in dieser Region, doch davon betroffen waren Kundinnen und Kunden weltweit.[5]

Die Aufgaben für die Sicherung von Informationen und IT-Equipment werden dementsprechend immer umfangreicher. Auch gesetzliche Vorgaben wie die DSGVO in Europa oder die NIS-Richtlinie geben den Unternehmen zusätzliche Aufgaben.

2
www.weforum.org/reports/the-global-risks-report-2018

3
www.bundeskanzleramt.gv.at/dam/jcr:aa859448-de81-44b2-af72-9a99376296d7/Cybersicherheit_Bericht2018.pdf

4
gvv.mpi-inf.mpg.de/projects/DeepVideoPortraits/

5
www.heise.de/newsticker/meldung/Blitzschlag-in-den-USA-stoert-Azure-Active-Directory-4155496.html

3. Internationale Entwicklung: Massive Kosten durch Cyberattacken

Welche Bedeutung der Bereich IT-Sicherheit inzwischen weltweit hat, zeigen diese Zahlen: Cyberangriffe gegen Unternehmen haben sich in den vergangenen fünf Jahren fast verdoppelt. Dementsprechend hat der Markt für CyberCrime massiv an Gewicht zugelegt: Im April 2018 wurde dieser bereits auf mehr als 1,5 Billionen US-Dollar geschätzt (Bromium 04/2018). Die durch CyberCrime verursachten Kosten betrugen hingegen 6 Billionen US-Dollar (Forbes 07/2017)

Symantec hat zudem erhoben, dass eine von 13 Web-Anfragen direkt zu Schadsoftware führt. Schadsoftware wird nun auch immer häufiger für Betriebssysteme abgesehen von Windows, zum Beispiel für Apple, gefunden. Die E-Mail-Spam-Rate steigt zudem stetig und liegt aktuell bei 55 Prozent. Die Anzahl von Attacken auf IoT-Geräte ist von 2016 auf 2017 um unglaubliche 600 Prozent gestiegen. Aber auch die Anzahl von gefundenen Schwachstellen wie EternalBlue oder Meltdown ist um 13 Prozent angestiegen, bei Industriesteuerung sogar um 29 Prozent.[6]

IBM hat eine globale Studie zum Thema der Kosten für Datenlecks („Data Breach“) veröffentlicht:[7]

→ Tabelle: rechte Seite

Dies stimmt auch mit einer internationalen Studie, durchgeführt von EY, überein, die das durchschnittliche Schadensausmaß eines Datenlecks mit etwa 3,2 Millionen Euro beziffert.[8] Beispiele für Datenlecks gibt es immer wieder. Im Jahre 2013 wurden beispielsweise bei einem Hackangriff 3 Milliarden Yahoo-Accounts gehackt, wo E-Mail-Adresse und Telefonnummern entwendet wurden. 2016 wurde ebenso das Unternehmen UBER Opfer eines Hackangriffs, in Zuge dessen ebenso sensible Daten wie Adressen und Klarnamen gestohlen wurde. Ein jüngerer Vorfall betrifft die Fluggesellschaft British Airways. Dieser wurden im Jahr 2018 persönliche Daten und Bankverbindungen zahlreicher Kundinnen und Kunden gestohlen. Betroffen waren Personen, die zwischen dem 21. August und dem 5. September 2018 über die Website und die App des Unternehmens Flüge buchten. Insgesamt waren rund 380.000 Bank- und Kreditkarten betroffen.[9]

Die Ausgaben für IT-Sicherheit steigen nicht nur wegen zunehmender Risiken, sondern auch durch neue Geschäftsbedürfnisse (z.B. Datenschutz) und Veränderungen in der Industrie (z.B. IoT). Gartner schätzt die Zunahme der Ausgaben im Jahr 2019 mit 8,7 Prozent (US$ 124 Mrd.) weltweit im Vergleich zu nur 3,2 Prozent für IT im Allgemeinen.[10]

6
www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

7
www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&

8
www.ey.com/Publication/vwLUAssets/EY_Global_Information_Security_Survey_2018_-_Oktober/$FILE/EY%20Global%20Information%20Security%20Survey%202018.pdf

9
www.forbes.com/sites/bishopjordan/2018/09/09/british-airways-hacked/#555cc04967ae

10
Gartner, “2019 Worldwide Security Spending Projection.”

Die Studie beziffert die Kosten für Vorfälle mit weniger als 10.000 gefährdeten Datensätzen mit 2,1 Millionen US-Dollar und für Vorfälle mit mehr als 50.000 gefährdeten Datensätzen mit 5,7 Millionen US-Dollar.

197 TAGE	ÜBER 1 MILLION US-DOLLAR
dauert es im Durchschnitt, bis ein Datenleck erkannt wird.	haben Unternehmen eingespart, die in weniger als 30 Tagen ein Datenleck beheben konnten.

Folgende Faktoren helfen, die Kosten für ein Datenleck zu erhöhen oder zu reduzieren:

KOSTENTREIBER (TOP 5)	KOSTENEINSPARUNGEN (TOP 5)
● Beteiligung Dritter (Outsourcing) ● Umfangreiche Cloud-Migration ● Compliance-Fehler ● Umfangreiche Nutzung mobiler Plattformen ● Verlorene oder gestohlene Geräte	● Sicherheitsvorfallsteam (Incident Response Team) ● Umfangreicher Einsatz von Verschlüsselung ● Einbindung in das Business Continuity Management ● Training der Teams ● Teilen von Informationen zu Bedrohungen

Situation in Österreich

4.1 Aktuelle Daten

Laut einer Studie von KPMG[12] werden auch in Österreich rund zwei von drei Unternehmen Opfer von Cyberkriminalität, wobei vor allem mittelständische Unternehmen und große Unternehmen im Fokus der Angreifer stehen. Angreifer zielen vor allem auf menschlich verursachte Schwachstellen ab. Zu den häufigsten Angriffsarten zählen Phishing, Malware/Ransomware/Schadsoftware und Social Engineering.

Vor allem die Angriffsmethoden Ransomware und Advanced Persistent Threats (APT) nahmen deutlich zu. Bei DDoS-Angriffen scheint der Höhepunkt der Vorjahre überwunden zu sein.

→ Tabelle: rechte Seite

Generell ist auch eine Zunahme von Cybercrimefällen zu verzeichnen, während bei konventionellen Straftaten ein Rückgang verzeichnet werden kann. Auch der Trend zur Beeinflussung der öffentlichen Meinung beispielsweise bei Wahlen via Social Media Plattformen ist in Österreich evident.

Unternehmen der kritischen Infrastruktur sowie der Cybersicherheitsbranche in Österreich reagieren auf die ständig steigende Bedrohung mit höheren Budgets für Maßnahmen zur Erhöhung der Cybersicherheit sowie eine laufende Implementierung neuer Sicherheitsmaßnahmen. Darüber hinaus ist ein Trend erkennbar, das Informationssicherheits- und Datenschutz-Personal aufzustocken.

Eine Einschätzung von Cybersicherheitstrends für 2018 zeigt sich in der Umfrage für den Bericht „Cyber Sicherheit 2018“:

- Die Gefährdungslage ist im Steigen begriffen. Angriffe werden komplexer und häufiger. Die Hauptmotivation hinter den Angriffen ist in der Monetarisierung zu suchen.
- Cloud Security wird zu einem entscheidenden Thema. Es ist eine zunehmende Abhängigkeit der Unternehmen von den Cloud-Anbietern zu erwarten.
- Netz- und Informationssystemsicherheitsgesetz (NIS-G) und Datenschutzgrundverordnung (DSGVO) werden erhebliche Anforderungen an Unternehmen stellen.
- Die Bedeutung organisatorischer Maßnahmen (z.B. Risikomanagement) wird künftig gegenüber rein technischen Maßnahmen zunehmen.

Laut einem Bericht des Bundeskriminalamts verzeichnete die Anzahl an CyberCrime-Delikten 2017 im Vergleich zu 2016 einen Anstieg um mehr als 52,6%. Brisante Vorfälle der letzten Jahre, in welche österreichische Institutionen direkt oder indirekt involviert waren, sind gemäß dem Bericht des Bundeskanzleramts für Cyber-Sicherheit[11] beispielsweise:

- WannaCry (05/2017): Ransomware, mittels welcher Zielsystem infiziert und deren Festplatteninhalt verschlüsselt wurde. Gegen Zahlung von Lösegeld wurden diese wieder entschlüsselt. Mehrere Länder europaweit waren betroffen.
- NotPetya (07/2017): Ebenfalls Ransomware, mittels welcher Unternehmen, die Geschäftsbeziehungen zur Ukraine unterhalten, infiziert wurden. Ziel des Angriffes war eine gezielte Sabotage der Infrastruktur der Ukraine.
- Nationalistische Hackergruppen (seit 08/2016): Mehrere österreichische Einrichtungen der kritischen Infrastruktur wurden Opfer von DDoS-Angriffen durch ausländisch nationalistische Hackergruppen. Betroffen waren unter anderem die österreichische Nationalbank sowie die Webseiten verschiedener Ministerien und des Parlaments.

11
www.bundeskanzleramt.gv.at/dam/jcr:aa859448-de81-44b2-af72-9a99376296d7/Cybersicherheit_Bericht2018.pdf

12
https://home.kpmg/at/de/home/insights/2018/05/cyber-security-studie-oesterreich-2018.html

Angriffsmethoden erklärt

RANSOMWARE	Ransomware sind Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln. Die Täter erpressen ihre Opfer, indem sie deutlich machen, dass der Bildschirm oder die Daten nur nach einer Lösegeldzahlung wieder freigegeben werden. Die Cyber-Erpresser spielen mit der Angst der Menschen und bereichern sich so auf deren Kosten.
ADVANCED PERSISTENT THREATS (APT)	Ein „Advanced Persistent Threat“ ist ein gezielter Angriff auf ein oder wenige Opfer, bei dem der Angreifer sehr zielgerichtet vorgeht. Er nimmt einen großen Aufwand auf sich, um nach dem ersten Eindringen in einen Rechner weiter in das lokale Netz des Opfers vorzudringen, wo er möglichst lange unentdeckt bleiben will, um über einen längeren Zeitraum Daten auszuspähen oder anderweitig Schaden anzurichten.
DDOS	Bei einer Distributed Denial-of-Service-Attacke (DDoS) greifen mehrere Computer gleichzeitig und im Verbund (Botnetze) eine Webseite oder eine ganze Netzinfrastruktur an. Dies kann sehr schnell zum Ausfall der Server führen. In einigen Fällen dient der Angriff als Ablenkung, während eines größeren Datendiebstahls.

4.2 Kein „Plan B“

So kommen auf das gesamte Wirtschaftssystem große Herausforderungen zu. „Wir sind kaum auf mögliche strategische Schockereignisse vorbereitet. In vielen Bereichen fehlt uns ein Plan B, um mit größeren Störungen und Totalausfällen sinnvoll umzugehen. Der erste Schritt beginnt mit dem Wissen um diese Bedrohungen“, ist Herbert Saurugg von der Cyber Security Austria (CSA) überzeugt.

Durch die Vernetzung gesamter Ökosysteme steige auch die Abhängigkeit von Energie und Informationen. „Somit können einfache Fehler enorme Folgen haben und Unfälle auslösen. Selbst die Energie-, Wasserversorgung, Kommunikation bzw. die gesamte Infrastruktur kann gefährdet werden“, warnt Herbert Dirnberger von CSA.

In den letzten Jahren wurden vermehrt Industriesysteme angegriffen und „Triton“ zeigt, dass Angriffe auf Industrieanlagen auch gezielt die Safety-Systeme betreffen können. „Angreifer von morgen werden sich nicht damit begnügen, Schwachstellen in existierenden Systemen zu finden, sondern aktiv daran arbeiten, dass Schwachstellen im Engineering-Prozess eingebaut werden“, erklärt Edgar Weippl, Forschungsleiter von SBA Research.

Sebastian Bachmann von Ikarus Security Software richtet den Fokus auf einen besonders kritischen Bereich: „Allein in den letzten Jahren kam es verstärkt zu groß angelegten Online-Banking-Betrugsfällen, die in dieser Form noch nie dagewesenes Potenzial der Malware-Branche zeigten. Oft wissen selbst Administratorinnen und Sicherheitsexperten nicht, wie mit den neuen Gefahren umzugehen ist.“

4.3 Engagement verstärkt

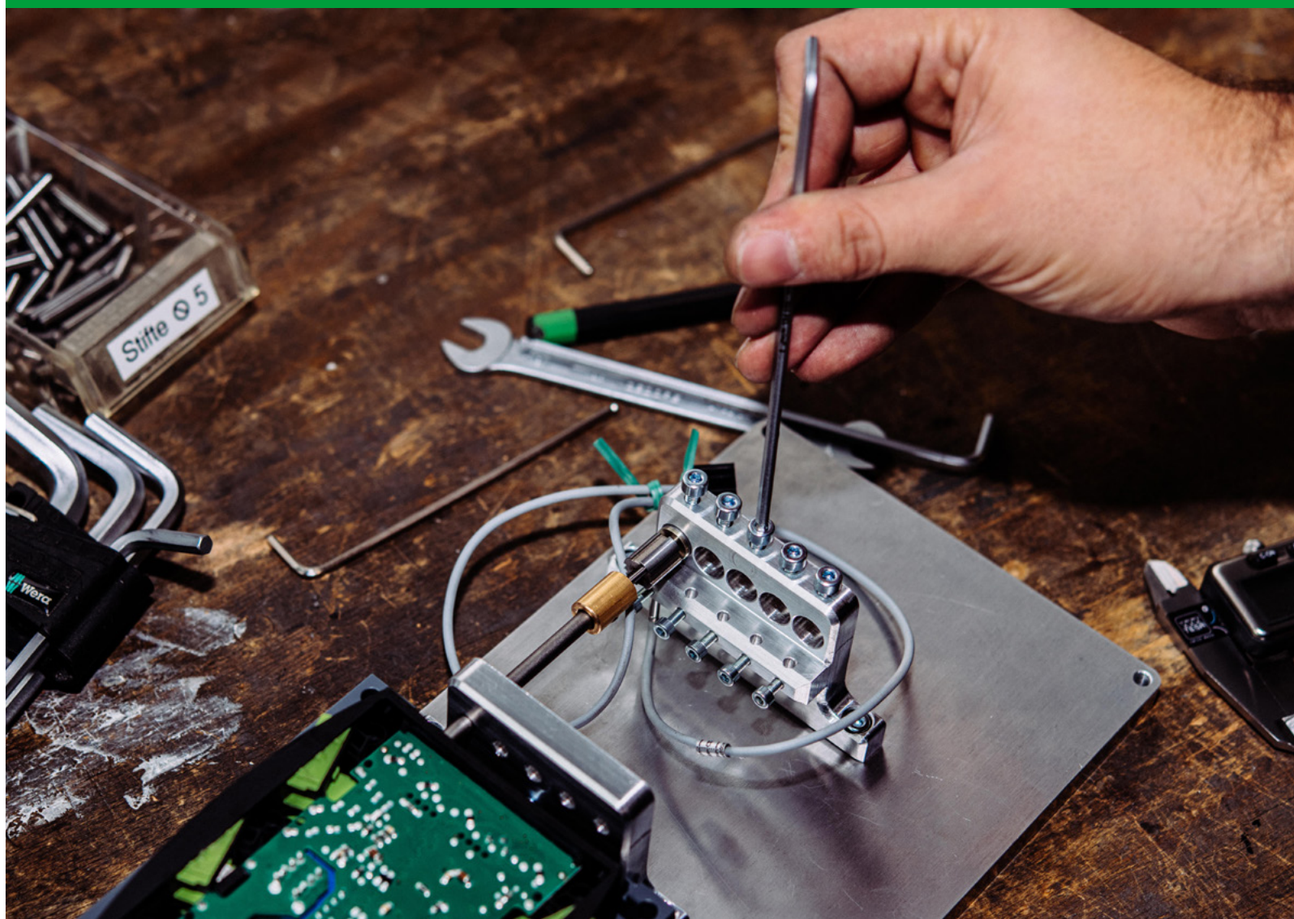
Wie wichtig diese neuen Bedrohungen inzwischen genommen werden, zeigen zahlreiche Initiativen verschiedener politischer, wissenschaftlicher sowie zivilgesellschaftlicher Organisationen:

Mit der „Österreichischen Strategie für Cyber Sicherheit“[13] wurde von der österreichischen Bundesregierung im März 2013 ein umfassendes Konzept zum Schutz des Cyberraums und der Menschen im virtuellen Raum beschlossen. Im „Bericht Cyber Sicherheit 2018“[14] sind die aktuellen Bedrohungen sowie die nationalen und internationalen Entwicklungen zusammengefasst. Darin ist von einer signifikanten Steigerung der Aktivitäten in den Bereichen Cyberspionage und Cyberkriminalität die Rede. Insbesondere die Angriffe im Bereich Ransomware werden in den nächsten Jahren weiter beträchtlich ansteigen.

Der gemeinnützige Verein Cyber Security Austria (CSA) wiederum hat das Ziel, eine Sensibilisierung für die Thematiken der IT-Security in Österreich zu schaffen. Dabei will dieser unterschiedliche Interessensvertreter aus den Bereich Politik, Wirtschaft, Wissenschaft, aber auch die Gesellschaft an sich ansprechen. Die Aktivitäten von Cyber Security Austria umfassen diverse Publikationen, Vorträge und Projektmitarbeiten, in welchen bereits vorhandenes Wissen zu IT-Security vernetzt und an andere weitervermittelt wird.

Am E-Day, einer der bekanntesten Veranstaltungen der Wirtschaftskammer Österreich, sowie der Telefit-Roadshow für Kleinere und Mittlere Unternehmen steht IT-Sicherheit regelmäßig am Programm. Speziell an Kinder, Jugendliche, Eltern und Lehrende richtet sich die österreichische Informations- und Koordinierungsstelle Saferinternet.at. Sie unterstützt Internetnutzer mit Tipps und Hilfestellungen bei der sicheren Nutzung von Internet, Handy und Computerspielen.

Das Computer Emergency Response Team Austria (CERT.at) fungiert als Ansprechpartner für IT-Sicherheit im nationalen Umfeld. Es vernetzt andere CERTs und CSIRTs (Computer Security Incident Response Teams) aus den Bereichen kritische Infrastruktur sowie Informations- und Kommunikationstechnik (IKT) und gibt Warnungen und Tipps für KMUs heraus. Das CERT der Stadt Wien (Wien CERT) wird durch die Magistratsabteilung 01 - Wien Digital betrieben.



13
www.bmi.gv.at/504/files/130416_strategie_cybersicherheit_WEB.pdf

14
https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment.html

5.1 Anzahl und Struktur

Wien ist Österreichs wichtigster Standort für Informationstechnologie und damit auch für IT-Sicherheit[15]. Viele Unternehmen bieten inzwischen Dienstleistungen in diesem Bereich an, wobei etwa 40 Betriebe, einen maßgeblichen Anteil ihres Umsatzes in diesem Bereich lukrieren bzw. eigene Forschung und Entwicklung betreiben.

Ein seit Jahren etabliertes Unternehmen ist die Ikarus Security Software GmbH. Sie entwickelt eigenständige Produkte, vor allem im Bereich Netzwerksicherheit, industrielle Sicherheit sowie Endpoint Security. Ein weiteres entwickelndes und innovatives Unternehmen ist das auf starke Authentisierung spezialisierte und international aktive Unternehmen Cryptas. Dieses bietet professionelle Lösungen im Bereich der Zugangssicherung, Integritätssicherung sowie der digitalen Identität an. Andere Unternehmen haben sich auf spezielle Aspekte der IT-Sicherheit spezialisiert: Das Wiener Unternehmen KiwiSecurity[16] liefert beispielsweise Software für Videoanalyse im Hochsicherheitsbereich und machte vor allem durch seine Lösung für Videoüberwachung unter gleichzeitigem Schutz der Privatsphäre international auf sich aufmerksam. T3K-Forensics[17] hat sich auf den Bereich digitaler Forensik spezialisiert, während RadarServices[18] u.a. Lösungen im Bereich IT-Security Monitoring anbietet.

Neben seinen Aktivitäten als Forschungseinrichtung bietet SBA Research auch Dienstleistungen zu Security-Themen an. Es agiert in einem Netzwerk nationaler und internationaler Spezialisten, deren Expertise vor allem im technischen Bereich legt. SBA Research wurde 2006 von der Technischen Universität Wien, der Technischen Universität Graz und der Universität Wien gegründet. In den letzten Jahren sind die Wirtschaftsuniversität Wien, das AIT Austrian Institute of Technology und die Fachhochschule St. Pölten als akademische Partner beigetreten. SBA Research ist mit mehr als 100 Mitarbeiterinnen und Mitarbeitern mittlerweile das größte Forschungszentrum Österreichs, das sich exklusiv mit Informationssicherheit beschäftigt. SBA ist ein COMET-Zentrum. Diese Zentren werden vom Bund und den Bundesländern gemeinsam im Verhältnis 2 Anteile des Bundes zu 1 Anteil der Bundesländer gefördert. Für Wien fördert die Wirtschaftsagentur Wien. Derzeit unterstützt die Wirtschaftsagentur 15 COMET Zentren und Projekte.

Cyan Network Security hat sich auf Proxy-Technologie und Web-Filter-Lösungen spezialisiert. Bacher Systems gehört mit rund 100 Mitarbeitern zu den größeren Anbietern und weist für IT-Security ein umfassendes Angebot auf. Es reicht von Lösungen im Bereich Privileged Access Security, Data Security, Mobile Security über Cloud Security und Network Security, Risikomanagement bis hin zu SIEM (Security Information & Event Management) Systemen.

Die Entwicklung in Wien folgt dem internationalen Trend der Spezialisierung in der IT-Sicherheitsbranche. Neben der traditionellen IT-Sicherheit für Firmennetze haben sich zuletzt Angebot und Nachfrage nach Sicherheit für den mobilen Bereich, in industriellen Umgebungen sowie im Bereich „Internet-der-Dinge“ entwickelt. Die Abgrenzung von Beratungsunternehmen zu Anbietern und Entwicklern eigener Lösungen ist dabei fließend. Die Experts Group IT-Security des Fachverbandes Unternehmensberatung und IT (UBIT) der Wirtschaftskammer Österreich verweist auf die große Zahl an Ein-Personen-Unternehmen in der Branche. Diese – meist spezialisierten – Einzelkämpfer im Bereich IT-Security seien zwar zum Großteil Dienstleister, allerdings verschwimme die Grenze zusehends. Das Adaptieren für die Kundenumgebung hat auch seinen Entwicklungsanteil. Hier sind die Übergänge durchaus nahtlos.

Die Spezialisierung auf Aspekte der IT-Sicherheit ist auch eine Folge des hohen Know-hows, das für IT-Sicherheit notwendig ist. Es dürfte inzwischen über 200 tatsächliche Security-Expertinnen und -Experten in Wien geben, die sich zumeist auf spezielle Aspekte fokussieren. Markus Klemen, Geschäftsführer von SBA Research führt aus: „Der Mangel an hochqualifizierten Expertinnen und Experten im Cyber Security Bereich wird in den nächsten Jahren noch zunehmen, als Wiener Forschungszentrum wollen wir diese Herausforderung gemeinsam mit unseren Partnerinstitutionen zukünftig noch stärker adressieren, etwa durch spezielle Kursformate. Dabei wollen wir auch den Fokus noch stärker auf die Förderung von Frauen in diesem Bereich legen, Expertinnen im IT-Sicherheitsumfeld sind leider immer noch ausgesprochen rar.“ Joe Pichlmayr von Ikarus bestätigt dies und verweist auf das Know-how und spannende Projekte rund um das Kompetenzzentrum SBA Research (siehe Kapitel „Ausbildung, Forschung und Netzwerke“).

Ein großer Vorteil Wiens zu anderen Ländern oder Städten ist, dass es ein sehr enges Netzwerk der Expertinnen und Experten zu unterschiedlichen Security-Themen gibt, egal ob von Behörden-, Industrie- oder Forschungsseite. Viele Akteurinnen und Akteure kennen einander gut und arbeiten in verschiedenen Vereinen oder Plattformen häufig miteinander. Dies erleichtert die Vermittlung von Kontakten und bietet wichtige Vorteile bei der Abwehr größerer Attacken. Eine wichtige Rolle bei Vernetzung und Kompetenzförderung in Wien stellen öffentliche Initiativen wie das Computer Emergency Response Team (CERT) dar.[19]

Die Stadt Wien reagiert in der Digitalen Agenda Wien ebenfalls auf aktuelle Entwicklungen: „Die zunehmende Digitalisierung sämtlicher Services und Prozesse macht es wesentlich, das Vertrauen der Bürgerinnen und Bürger in die Sicherheit unserer IKT-Systeme, Daten und Dienste zu gewährleisten.“[20]

15
www.wien.gv.at/wirtschaft/standort/pdf/ikt-standort.pdf

16
www.kiwisecurity.com/?lang=de

17
www.t3k-forensics.com/de

18
www.radarservices.com/de

5.2 Kundinnen und Kunden

Die Kundschaft der IT-Security Unternehmen in Wien erstreckt sich über ein sehr breites Feld. Neben Kleinstunternehmen, wo auch diverse Anwaltskanzleien dazuzuzählen sind, nehmen auch zahlreiche Großunternehmen wie Siemens AG Österreich und Behörden diese in Anspruch.

Trotz der wachsenden Sensibilisierung für IT-Security in Unternehmen besteht dennoch weiterhin großer Aufklärungsbedarf. Insbesondere Klein- und Mittelunternehmen, die nur eine geringe Anzahl an Mitarbeitern beschäftigen, sind sich der Wichtigkeit der Thematik bei ihren eigenen Unternehmen oftmals nicht bewusst. Ebenso spielen die im Vergleich zu großen Firmen geringeren Ressourcen eine wichtige Rolle für die mangelnde Auseinandersetzung mit IT-Sicherheit. Laut Markus Klemen, Geschäftsführer von SBA Research, führt dies dazu, dass Klein- und Mittelunternehmer IT-Sicherheitsmaßnahmen oft als eine Art „Luxus“ betrachten würden, die am Ende von Projekten bestenfalls in Form von Penetration Tests oder Sicherheitsüberprüfungen zur Anwendung kommen. „Eine frühzeitige Einbindung von Sicherheitsüberlegungen wäre kostentechnisch wesentlich sinnvoller, da Architekturfehler vermieden werden können, die zu einem späteren Zeitpunkt nur mit erheblichem Mehraufwand – wenn überhaupt – beseitigt werden können. Die Bereitschaft dazu ist noch nicht ausreichend ausgeprägt.“

Als Vorteil für die Wiener IT-Sicherheitsunternehmen im Wettbewerb gilt vor allem die Nähe zur Kundschaft. So kann ein für diesen Bereich besonders wertvolles Vertrauensverhältnis aufgebaut werden, das – insbesondere, wenn sensible Daten und Bereiche betroffen sind – als enorm wichtig gilt. Als bedeutender Faktor ist natürlich auch die Agglomeration von internationalen Firmen und Organisationen in Wien zu sehen.

19
www.cert.at

20
https://digitales.wien.gv.at/site/daw2025/

„In diesem Bereich sind Vertrauen und der persönliche Kontakt wesentlich“
erklärt Edgar Weippl (SBA Research).

Die Qualität des Ausbildungsangebots und der Forschungseinrichtungen im Bereich IT-Security hat sich in Wien von einer bereits guten Position ausgehend zuletzt weiter gebessert. Neben zentralen Institutionen wie der Technischen Universität (TU) Wien gibt es umfangreiche Angebote unter anderem von Fachhochschulen.

Die TU Wien hat durch eine neue Professur im Security-Bereich[21] (Prof. Matteo Maffei) ihr Angebot wesentlich ausgebaut. Die Schwerpunkte liegen auf Kryptographie, Websicherheit, mobilen Systemen sowie im Bereich Anwendungen der Kryptographie für elektronische Währungen, Cloud und Datenanalyse unter Bewahrung der Privatsphäre. Die TU Wien reiht sich beim internationalen Hacker-Wettbewerb iCTF (International Capture The Flag) regelmäßig unter die besten der Welt ein. Sie ist auch am International Secure Systems Lab (iseclab), einer Vereinigung von fünf internationalen System- und Sicherheitsforschungslaboratorien, beteiligt.

Die FH Campus Wien verfügt über ein Kompetenzzentrum IT-Security, die FH Technikum Wien bietet einen F&E-Schwerpunkt Secure Services, eHealth & Mobility. Beide FHs bieten Master-Studiengänge zum Thema an. Berufsbildende Höhere Schulen, etwa das TGM oder die HTBLVA Spengergasse runden das Ausbildungsangebot ab.

SBA Research ist das größte österreichische Kompetenzzentrum für angewandte Forschung im Bereich IT-Security. Es arbeitet u.a. eng mit der TU Wien, weiteren Universitäten und einem großen Netzwerk verschiedener Unternehmen zusammen. Über 100 Forscherinnen und Forscher analysieren die IT-Sicherheit von Systemen, von klassischer Unternehmens-IT bis zur Sicherheit von Produktionssystemen. Zahlreiche Veranstaltungen und Kurse bieten Interessierten einen einfachen und soliden Einblick in den Stand von Wissenschaft und Technik.

Eine fixe Größe in der heimischen Forschungslandschaft ist das AIT Austrian Institute of Technology, das ein eigenes Zentrum für Digital Safety & Security[22] betreibt. Es widmet sich schwerpunktmäßig der Sicherstellung von operativer Effizienz und Zuverlässigkeit aller kritischen Infrastrukturen und der Entwicklung und Bereitstellung von zukunftsweisenden Technologien.

Wichtige F&E-Themen am AIT adressieren u.a. Command und Control Systeme für den Einsatz im Krisen- und Katastrophenmanagement, Cybersicherheit (AIT Cyber Range), Big Data und Blockchain-Technologien, sichere und zuverlässige Systeme, neueste Sensortechnologien und Systeme zum Schutz kritischer Infrastrukturen und digitales Identity Management durch modernste Biometrie-Sensorik, intelligente Kameras und Videoanalyse, neue Sensortechnology und Sicherheit auf der physischen Ebene.

Mit dem Förderprogramm für Sicherheitsforschung KIRAS gibt es eine gezielte Initiative, die den Schutz kritischer Infrastrukturen in den Vordergrund rückt. KIRAS unterstützt nationale Forschungsvorhaben, die die Sicherheit für alle Mitglieder der Gesellschaft erhöhen. Dieses Ziel verfolgt auch „A-SIT, das Zentrum für sichere Informationstechnologie“. A-SIT ist ein gemeinnütziger Verein institutioneller Mitglieder mit öffentlich-rechtlichem Charakter.[23]

6.1 Vienna Cyber Security and Privacy Research Center (VISP)

IT Sicherheit und der Schutz privater Daten gehören zu den großen Herausforderungen, die der fundamentale digitale Wandel mit sich bringt. Vor allem die Sicherheit von kritischen Infrastrukturen, die Bekämpfung von Fake News und die Organisation von zuverlässigen E-Government Services, die Sicherheit für private Daten garantieren, sind für die Stadt Wien von sehr großer Bedeutung.

21
www.secpriv.tuwien.ac.at/home/

22
www.ait.ac.at/ueber-das-ait/center/center-for-digital-safety-security/

23
www.a-sit.at/

Auch die Wirtschaft steht vor der Herausforderung, sich gegen aktuelle Bedrohungen zu rüsten. Alleine in Österreich entsteht durch Cyberspionage jährlich ein Schaden im Wert von 1,6 Mrd. EUR (Bericht des Österreichischen Verfassungsschutzes aus dem Jahr 2017).

Gleichzeitig eröffnen diese Herausforderungen die Chance, innovative Lösungen zu entwickeln und erfolgreich auf den Markt zu bringen. Dadurch entstehen Wachstum und Beschäftigung. Das größte Innovationspotenzial ergibt sich dabei an der Schnittstelle zwischen den Disziplinen und Branchen.

Wien und die Vienna Region haben im Thema IT Security und Privacy eine ausgezeichnete akademische Basis. Alleine an der TU Wien, der Universität Wien und dem IST Austria, den drei Top-Institutionen in diesem Feld, gibt es derzeit 10 Professuren für Cyber Security and Privacy. Die genannten Forschungseinrichtungen haben erfolgreich 5 Grants des European Research Councils eingeworben – das ist im internationalen Vergleich einzigartig.

Die drei Institutionen bündeln seit 2020 ihre Aktivitäten nun unter einem gemeinsamen Dach, um sich noch besser zu koordinieren und international sichtbarer zu machen. Mit der Gründung des Vienna Cyber Security and Privacy Research Centers sollen folgende Ziele erreicht werden:

- Initiierung von institutionenübergreifenden international sichtbaren Forschungsaktivitäten
- Ausbildungsangebote für Security Expertinnen und Experten für Industrie und Wissenschaft
- Unterstützung für regionale Startups
- Ansiedlung von internationalen Firmen in diesem Feld.

Das VISP wird von der Wirtschaftsagentur Wien aus Mitteln des Strukturimpulsprogramms gefördert und hat die Antragsphase aktiv unterstützt.

6.2 Online Sicherheitsportal

Eine einfach erreichbare Informationsquelle bietet das Online Sicherheitsportal www.onlinesicherheit.gv.at. Diese strategische Maßnahme der nationalen IKT-Sicherheitsstrategie hilft Unternehmen bei der Identifikation von möglichen IT-Sicherheitsproblemen. Das Portal informiert ständig über aktuelle Sicherheitsbedrohungen, sowie Veranstaltungen und Publikationen zum Thema.

Das Portal wird vom Zentrum für sichere Informationstechnologie – Austria (A-SIT) im Auftrag des Bundesministeriums für Digitalisierung Wirtschaftsstandort betrieben. Es bietet unabhängigen Rat und Hilfestellung für mehr Sicherheit in der digitalen Welt.

Das Portal bietet eine Übersicht über mögliche Gefährdungen von der Nutzung von konventionellen Computern bis zu mobilen Geräten. Es gibt auch Auskunft über richtiges online Verhalten beim Online-Shopping oder -Banking und widmet einen eigenen Abschnitt des richtigen Umgangs von Kindern mit dem Internet. Auch das zunehmend wichtige Thema „Internet der Dinge – Internet of Things“, d.h. der online vernetzten Alltagsgegenstände wird aufgegriffen.

6.3 CryptoPartys und Events

In Wien finden regelmäßig sogenannte CryptoPartys statt, bei denen es um einen niederschwelligen Zugang zum Thema Privatsphäre im Internet, Kryptographie und beachtenswerte Dinge geht. Dabei werden unter anderem folgende Themen beleuchtet: Verschlüsselung von E-Mails, Festplatten, Chat und Telefonie, anonymes Websurfen, aber auch anonymes Veröffentlichen.[24]

Auch der gemeinnützige Verein Cyber Security Austria (CSA) widmet sich der öffentlichen Vermittlung von Erkenntnissen im Bereich der IT-Sicherheit, u.a. durch öffentliche Veranstaltungen und Publikationen.[25]

Schon 2012 wurde die Austria Cyber Security Challenge[26] (ACSC) ins Leben gerufen (www.verbotengut.at), welche sich auf Initiative der CSA mittlerweile auch zu einer großen European Cyber Security Challenge (ECSC) weiterentwickelt hat (www.europeancybersecuritychallenge.eu). Die ACSC ist Österreichs erste IT Security Talentsuche zur Rekrutierung junger, qualifizierter Menschen. Diese Gruppe stellt in Zukunft das personelle Rückgrat zur Abwehr von nationalen Cyberangriffen dar. Im Rahmen der Challenge sollen junge Talente entdeckt und prämiert werden.

Das AIT veranstaltet das „International Digital Security Forum[27]“ unter dem Motto: „Global Discussion for a Connected World“. Neben Präsentationen und Gesprächen bieten zahlreiche Aussteller Einblicke in aktuelle Entwicklungen auf dem Gebiet Cyber Security.

SBA organisiert die jährliche Konferenz „Sec4Dev – Conference & Bootcamp[28]“. Sie hat einen starken Fokus auf praktische, anwendbare, hands-on sowie sicherheitsrelevante Inhalte für Personen, die in der Softwareentwicklung tätig sind. Ziel ist es, Sicherheit zu einem der relevantesten Themen in der Welt der Softwareentwicklung zu machen.

24
www.cryptoparty.at/start

25
www.cybersecurityaustria.at/

26
https://verbotengut.at/ueber-uns

27
https://idsf.io/

28
https://sec4dev.io/

Aufklärungsbedarf, insbesondere bei Klein- und Mittelbetrieben, die sich der Problematik auch für ihr eigenes Unternehmen oftmals nicht bewusst sind. Hier gilt es gezielt Maßnahmen zu treffen, die den Unternehmen die auf lange Sicht gesehen großen finanziellen Vorteile von Sicherheitsinvestitionen in ihren eigenen Betrieb verdeutlichen sollen.

Umstritten ist unter Experten, ob sich durch das Hineinwachsen der IT in andere Sektoren – Schlagworte dazu: cyberphysikalische Systeme, Blockchain/Smart Contracts, Usability – kurzfristig neue Geschäftsmöglichkeiten für die Branche ergeben. Während manche darauf pochen, dass die Zusammenarbeit interdisziplinärer wird und sich Spezialistinnen, die Steuerungs- oder Heizungsanlagen bauen, mit IT-Security-Experten vernetzen, sprechen andere von „Wunschdenken". Längerfristig scheinen sich aber durchaus neue Optionen für die Branche aufzutun. Edgar Weippl, Leiter des CD-Labors SQI, ist davon überzeugt, dass der Engineering-Prozess von Industrieanlagen von den Erfahrungen der Softwarebranche der letzten zehn Jahre profitieren kann:

> „Die Qualität und die Sicherheit von Software hat im letzten Jahrzehnt dramatisch zugenommen und Anlagenbauer sollten bei der Einführung eines Secure Development Lifecycles auf diese Erfahrungen zurückgreifen, um die Engineering-Prozesse besser abzusichern."

Die Anzahl an Cyberattacken wird mit der fortschreitenden Technologisierung und Vernetzung unserer Gesellschaft in Zukunft weiterhin dramatisch ansteigen. In Hinblick auf den Wirtschaftsstandort Wien gilt es dabei effektive Maßnahmen zu ergreifen, die einerseits den Schutz der kritischen Infrastruktur und andererseits den Schutz von sensiblem Wissen – Stichwort Wirtschaftsspionage – zum Ziel haben. Um dies zu gewährleisten, müssen mehrere Dinge gewährleistet werden:

Zunächst gilt es die Investitionen und Kapazitäten in den Ausbildungsbereich für IT-Security weiterhin zu erhöhen. Insbesondere Hochschulausbildungen an FHs und den Universitäten gilt es in diesem Bereich massiv zu fördern, um Unternehmen und Behörden mit fachlich kompetenten Mitarbeiterinnen und Mitarbeitern zu versorgen. Im Raum Wien sind beispielsweise die Universität Wien, die Technische Universität Wien sowie die FH Technikum Wien und FH Campus Wien enorm wichtige Ausbildungsstätten, die ebenso in der Forschung aktiv sind und wiederum durch die Forschungsexpertise anderer Forschungseinrichtungen wie SBA Research profitieren.

Wenngleich weitere Investitionen in eine gute Ausbildung ein wichtiges Fundament bilden, können sie den bereits bestehenden Fachkräftemangel dennoch bei weitem nicht beseitigen. Laut einem Bericht der Wirtschaftskammer lag die Anzahl der vakanten Stellen in den letzten Jahren bei ca. 5.000[29]. In diesem Zusammenhang gilt es effektive Konzepte auszuarbeiten, die qualifizierte Menschen aus anderen Ländern verstärkt anwerben sollen.

Die Awareness von Unternehmen zum Thema IT-Security ist merklich angestiegen. In vielen Unternehmen werden bereits zahlreiche Maßnahmen getroffen, um die Sicherheit ihrer Infrastrukturen und Daten zu gewährleisten. Nichtsdestotrotz besteht bei etlichen Unternehmen weiterhin massiver

29 www.kurier.at/wirtschaft/fachkraeftemangel-it-spezialisten-fuer-kmu-kaum-noch-leistbar/400357549

Die Wirtschaftsagentur Wien versteht sich als Netzwerk der Wiener IKT-Branche und unterstützt Unternehmen beratend aber auch beim Vertrieb und der Vernetzung untereinander. Veranstaltungen und Workshops zu Themenstellungen aus dem IKT-Bereich finden regelmäßig statt.

Zudem hilft die Wirtschaftsagentur Wien bei Betriebsansiedelungen oder Internationalisierungsangeboten. Auch für Gründerinnen und Jungunternehmer gibt es Hilfe im Startup Bereich. Kostenlose Workshops und Coachings zu Themen des unternehmerischen Alltags werden ebenso angeboten wie kleine, leistbare Büros.

Founders Labs[30]: Kostenloses Intensivtraining über mehrere Wochen zum Durchstarten.

8.1 Aktuelle Förderprogramme

Das Ziel der Wirtschaftsagentur Wien ist die kontinuierliche Entwicklung der internationalen Wettbewerbsfähigkeit durch Unterstützung der Wiener Unternehmen und ihrer Innovationskraft, sowie durch eine nachhaltige Modernisierung des Wirtschaftsstandortes. Um dieses Ziel zu erreichen, bietet die Wirtschaftsagentur Wien allen Wirtschaftstreibenden in Wien kostenlose Beratung zu den Themen Unternehmensgründung, Betriebsansiedlung oder -erweiterung, Unternehmensförderung und -finanzierung. Darüber hinaus werden auch Netzwerkkontakte in die Wiener Wirtschaft zur Verfügung gestellt.

Die Wirtschaftsagentur Wien unterstützt Unternehmen, die Forschungs- und Entwicklungsprojekte durchführen, mit individueller Beratung und monetärer Förderung. Je nach Bedarf erhalten sie Informationen über Förderungen, Finanzierungsmöglichkeiten, mögliche Entwicklungspartnerinnen, Forschungsdienstleister, oder Forschungsinfrastruktur.

○ Innovation[31]:

Das Förderprogramm Innovation unterstützt bei der Entwicklung von neuen oder deutlich verbesserten Produkten, Dienstleistungen und Verfahren oder der Durchführung organisatorischer Innovationen.

○ Wien Digital[32]:

Das Förderprogramm Wien Digital unterstützt bei der Umsetzung von Digitalisierungsvorhaben oder Ideen zur Optimierung betrieblicher Abläufe.

○ F&E Kooperationsanbahnung[33]

unterstützt Unternehmen, die nationale oder internationale Forschungs- und Entwicklungskooperationen anbahnen.

Alle Förderprogramme der Wirtschaftsagentur Wien finden Sie hier:
https://wirtschaftsagentur.at/foerderungen/programme/

30 https://wirtschaftsagentur.at/gruenden-und-wachsen/founders-lab-future-technologies/

31 https://wirtschaftsagentur.at/foerderungen/programme/innovation-90/

32 https://wirtschaftsagentur.at/foerderungen/programme/wien-digital-110/

33 https://wirtschaftsagentur.at/foerderungen/programme/f-e-kooperationsanbahnung-82/

9. Unternehmen aus Wien

Wir bieten Ihnen mit der alphabetischen Auflistung[34] auf den folgenden Seiten einen Überblick über ausgewählte Unternehmen aus Wien, die im Bereich IT-Security Leistungen anbieten.

Unternehmen und Forschungseinrichtungen

UNTERNEHMEN	BESCHREIBUNG	KONTAKT/WEBSEITE
A.SYS	A.SYS bietet ein breites Portfolio im Bereich Cybersecurity an. Das Angebot reicht hierbei von Business Antivirussoftware, DNS Security Service bis hin zu einer Plattform, die sensible Unternehmensinformationen im Darknet und Deep Web aufspüren kann.	Seitenhafenstraße 15/205 1020 Wien T +43 1 585 76 36 office@asys.at Ansprechperson: Hans Christian Singhuber www.asys.at
A1 CYBER RANGE	Als größter österreichischer Telekommunikationsanbieter weist A1 auch im Bereich der IT-Security ein umfangreiches Angebot auf. Neben eigenen Firewallsystemen und Software zur sicheren Datenübertragung bietet das Unternehmen ebenso eine Trainingsakademie an, wo IT-SpezialistInnen von Unternehmen ihre Skills weiter intensivieren können.	Lassallestraße 9 1020 Wien T +43 800 664 444 664 business.loesungen@a1.net www.a1.net/a1-cyber-range
AUSTRIAN INSTITUTE OF TECHNOLOGY	Das Austrian Institute of Technology (AIT) ist die größte außeruniversitäre Forschungseinrichtung Österreichs. Diese beschäftigt sich mit verschiedenen Themen im IT-Bereich, so auch mit Cybersecurity. AIT betreibt einerseits Forschung zur Entwicklung neuer Sicherheitstechnologien, anderseits werden bereits etablierte Technologien und Tools zur Stärkung kritischer Infrastrukturen angeboten und im Rahmen von speziellen Workshops und Schulungen vermittelt.	Giefinggasse 4 1210 Wien T +43 1 50550-4100 markus.kommenda@ait.ac.at www.ait.ac.at/dss
ANOVIS	Das Unternehmen Anovis ist seit dem Jahr 2004 im Bereich IT-Security tätig und kann auf ein umfangreiches Angebot verweisen. Neben allgemeinen Beratungstätigkeiten unterstützt Anovis bei Bedarf auch bei der gesamten Konzeption, Implementierung sowie beim Betrieb von Netzwerk- und Datacenter-Infrastrukturen.	Rennweg 97–99 1030 Wien T +43 1 7124070 office@anovis.com www.anovis.com

34
Diese Liste stellt keinen Anspruch auf Vollständigkeit

UNTERNEHMEN	BESCHREIBUNG	KONTAKT/WEBSEITE
A-TRUST	A-Trust ist ein qualifizierter Vertrauensdiensteanbieter für elektronische Zertifikate und bietet verschiedene Lösungen in diesem Bereich an. Diese reichen von der Handy-Signatur, über diverse Software-Zertifikate bis hin zu Registrierkassenzertifikaten.	Landstraßer Hauptstraße 1b The Mall E02 1030 Wien T +43 1 71321510 office@a-trust.at www.a-trust.at
BACHER SYSTEMS	Das Unternehmen Bacher Systems bietet für IT-Security ein umfassendes Angebot. Es reicht von Lösungen im Bereich Privileged Access Security, Data Security, Mobile Security über Cloud Security und Network Security, Risikomanagement bis hin zu SIEM (Security Information & Event Management) Systemen.	Wienerbergstr. 11/B9 (Turm B) 1100 Wien T +43 1 601260 info@bacher.at www.bacher.at
BECHTLE	Bechtle versteht sich als Anbieter ganzheitlicher Lösungen im Bereich der Cybersecurity. Das Portfolio des Unternehmens umfasst Beratungstätigkeiten im Bereich der Threat Prevention und der Informationssicherheit sowie Lösungen im Bereich der Application und Cloud Security.	Technologiestraße 8 1120 Wien T +43 1 570040 office.at@bechtle.com Ansprechpartner: Robert Absenger www.bechtle.com/at
BITMAN	Bitman verfügt bereits über eine langjährige Erfahrung im Bereich der IT-Security. Das Unternehmen bietet verschiedene Lösungen zur Entwicklung und Verwaltung sicherer und flexibler Systeme für seine KundInnen an. Ebenso bei plötzlich auftretenden Akutsituationen kann Bitman herangezogen werden.	Engerthstraße 227 1020 Wien T +43 664 524 9612 office@bitman.at www.bitman.at
BRAINLOOP AUSTRIA	Das international tätige Unternehmen Brainloop zeichnet sich durch eine breite Palette moderner Technologien im Bereich der IT-Security aus. Dazu zählen Firewallsysteme, eine 256-BIT-SSL/TLS-Verschlüsselung, sowie Dokumenten-Fingerprint-Technologie. Ebenso bietet das Unternehmen Hosting in ISO 270001-zertifizierten-Rechenzentren in mehreren Ländern Europas an.	Gonzagagasse 19/3 1010 Wien T +43 1 361 9790 info@brainloop.de www.brainloop.com/de-de
CERT.AT/ E-CERT/ GOVCERT	CERT.at ist das österreichische nationale CERT (Computer Emergency Response Team). Dieses fungiert als Ansprechpartner für IT-Sicherheit, vernetzt CERTs und CSIRTs (Computer Security Incident Response Teams) aus den Bereichen der kritischen Infrastruktur & IKT und unterstützt KMUs mit allgemeinen Warnungen und Tipps.	Karlsplatz 1/2/9 1010 Wien T +43 1 505641678 team@cert.at www.cert.at

UNTERNEHMEN	BESCHREIBUNG	KONTAKT/WEBSEITE
CHANGE-IT	Change-IT ist als Unternehmen im Bereich der Cybersecurity für KMUs tätig. Es werden ganzheitliche Lösungen unter anderem im Bereich der Application Security, Business Continuity bei Datenverlusten sowie Access Control zur Vereinfachung von Arbeitsabläufen angeboten.	Lerchenfelder Straße 70–72/5 1080 Wien T +43 699 17992940 office@change-it.at www.change-it.at/security
CORETEC	Das Unternehmen CoreTEC weist eine 100%ige Spezialisierung auf IT Security auf und kann dadurch ein hohes Maß an Qualität und Services anbieten. Dazu zählen beispielsweise verschiedene Penetration Tests, Beratungs- und Begleitungstätigkeiten von Firmen hinsichtlich ihrer Systemsicherheitspolitik, Security Trainings sowie Beratungen und Vorbereitungen zu ISO 27001 Zertifizierungen.	Ernst-Melchior-Gasse 24/DG 1020 Wien T +43 1 50372730 www.coretec.at
CRYPTAS	CRYPTAS hat sich innerhalb des IT-Security Bereichs auf starke Authentisierung spezialisiert. Das Unternehmen bietet dabei professionelle Lösungen im Bereich der Zugangssicherung (Mehrfaktorauthentisierung), Integritätssicherung (Datenverschlüsselung, digitale Signaturen) und digitalen Identität (Portalannmeldungen, Identity Federation) an.	Franzosengraben 8/4OG 1030 Wien T +43 1 355530 office@cryptas.com www.cryptas.com
CYAN	Das international agierende Unternehmen cyan kann auf eine hohe Vielfalt an Produkten auf Basis zukunftsorientierter Technologien im IT-Security Bereich verweisen. Ihre KundInnen sind dabei beispielsweise Versicherungen, Regierungen, Banken und Spieleanbieter. Sie bieten Lösungen im Bereich der OnNet Security, Personal Protection & Authentication an.	Wiedner Gürtel 13 1100 Wien office@cyansecurity.com www.cyansecurity.com
CSA	Cyber Security Austria (CSA) ist ein gemeinnütziger Verein mit dem Ziel, eine Sensibilisierung für die Thematik der IT-Security zu schaffen. Dabei will dieser unterschiedliche Stakeholder wie Politiker, Wirtschaftstreibende, Wissenschaftler, aber auch die Gesellschaft an sich ansprechen. Seine Aktivitäten erstrecken sich von Publikationen, über Vorträge bis hin zu Projektmitarbeiten, in welchen bereits vorhandenes Wissen vernetzt und vermittelt wird.	Blechturmgasse 11 1050 Wien office@cybersecurityaustria.at www.cybersecurityaustria.at

UNTERNEHMEN	BESCHREIBUNG	KONTAKT/WEBSEITE
CYBERTRAP	Das im Jahr 2015 gegründete Unternehmen CyberTrap ist Spezialist für Cyber-Security für Regierungsorganisationen und große Unternehmen. Mittels einer von ihnen entwickelten Deception-Lösung lassen sich Angriffe auf sensible IT-Systeme abhalten und dadurch entstehender Schaden vermeiden. Der Angreifer wird dabei ohne sein Wissen in eine eigene Umgebung umgeleitet, in welcher er dann überwacht werden kann.	Auerspergstraße 4/7 1010 Wien T +43 1 8904700 contact@cybertrap.com www.cybertrap.com
DELOITTE ÖSTERREICH	Das Unternehmen Deloitte zeichnet sich einerseits durch seine starke Internationalität und andererseits durch seine große Palette an unterschiedlichen Serviceleistungen aus. Im Bereich der Cyber-Security unterstützt Deloitte Unternehmen beispielsweise dabei, eine Risikoanalyse hinsichtlich ihrer IT-Systeme durchzuführen, rechtliche & sicherheitsbezogene Anforderungen in diesem Bereich zu erfüllen und ein umfassendes Identity & Access Management aufzubauen.	Renngasse 1/Freyung 1010 Wien T +43 1 537007950 office@deloitte.at Ansprechpartner: Mag. Alexander Ruzicka www2.deloitte.com/at/de
EXPRESSFLOW	expressFlow hat sich auf die Entwicklung mobiler Anwedungen im Bereich IT-Security spezialisiert. Durch ihre Applikation SecureBeam App können Dateien aus bestehenden Cloudspeichern verschlüsselt, in Stücke geteilt und dann als Datenblöcke an die jeweils bestehenden Cloudspeicher zufällig verteilt werden. Über Zugriffe und Änderungen an den jeweiligen Dateien informiert die App in Echtzeit.	Pater-Schwartz-Gasse 11A 1150 Wien contact@expressflow.com Ansprechpartner: DI Dr. Martin Vasko www.expressflow.com
FH CAMPUS WIEN	Die FH Campus Wien verfügt über ein Kompetenzzentrum IT-Security sowie den berufsbegleitenden Masterstudiengang IT-Security. Außerdem gibt es ein Cyber Security Team, welches sich mit Pentesting, Ethical Hacking, Capture-The-Flag-Wettbewerben und Kryptographie-Challenges beschäftigt.	Favoritenstraße 226 1100 Wien T +43 1 606 68 77-6600 office@fh-campuswien.ac.at www.fh-campuswien.ac.at/de/
FH TECHNIKUM	Die FH Technikum Wien bietet sowohl einen F&E-Schwerpunkt Secure Services, eHealth & Mobility als auch einen Masterstudiengang IT-Security an. Der Masterstudiengang IT Security veranstaltet jedes Jahr zusammen mit der Fakultät für Computer Science den Security Potpourri: eine Veranstaltung, bei der die neuesten Entwicklungen von Experten aus der Branche präsentiert werden.	Höchstädtplatz 6 1200 Wien T +43 1 333 40 77-0 its@fh-campuswien.ac.at www.technikum-wien.at

UNTERNEHMEN	BESCHREIBUNG	KONTAKT/WEBSEITE
GEKKO IT-SOLUTIONS	Seit mehr als 20 Jahren ist GEKKO it-solutions als Dienstleister im IT-Security Gebiet tätig. Sein Angebot erstreckt sich dabei vorrangig auf die Beratung und Betreuung von Daten im Bereich der Firewall Network Security, Verschlüsselungen, Disaster Recovery sowie allgemeinen Backups.	Wiegelestraße 10 1230 Wien T +43 1 710 5656510 office@gekko.at Ansprechpartner: Thomas Hofstätter www.gekko.at
HACKNER SECURITY INTELLIGENCE	Hackner Security Intelligence wurde 2010 mit dem Ziel gegründet, das bisherige Spektrum an IT Sicherheitsüberprüfungen um die Bereiche der physischen Sicherheit und Social Engineering zu erweitern. Das Angebot reicht dementsprechend von allgmeinen IT Pentration Tests, über Vulnerability Management, bis hin zu eigenen Security Trainings, in welchen MitarbeiterInnen von Unternehmen wichtiges Know-How zu IT-Security vermittelt werden.	Franz-Josefs-Kai 27/3B 1010 Wien T +43 1 2052300 office@hackner-security.com www.hackner-security.com/1/
HXS	Das Unternehmen HXS deckt eine große Palette unterschiedlicher Bereiche in der Business-IT-Welt ab. Hinsichtlich ihrer Cybersecuritylösungen bieten sie neben individuellen IT-Sicherheitsrisikoanalysen umfassende Firewall- & Antivirussysteme, Backups und ebenso Consulting Sessions zur Sensibilisierung.	Millergasse 3 1060 Wien T +43 1 3441344 office@hxs.at Ansprechpartner: Lorenz Bindhammer, BSc (WU) www.hxs.at
IKARUS SECURITY SOFTWARE	IKARUS Security Software weist ein umfassendes Angebot von Sicherheitsprodukten sowohl für Heimanwender als auch für Unternehmensnetzwerke auf. Die jeweiligen Anwendungen erstrecken sich hierbei auf die Bereiche Network Protection, Industrial Security sowie Endpoint Protection.	Blechturmgasse 11 1050 Wien T +43 1 589950 office@ikarus.at www.ikarussecurity.com/at/
INFRAPROTECT®	Fehlendes Sicherheitsbewusstsein und mangelnde Schutzvorkehrungen begünstigen in vielen KMUs Cyberangriffe. INFRAPROTECT® ist spezialisiert auf Risikoanalysen entsprechend geltender Normen und Gesetze. Darauf basierend werden punktgenaue Maßnahmenpläne erstellt sowie Mitarbeiter in Sachen Security Awareness und richtiges Verhalten in kritischen Situationen trainiert.	Ghegastraße 3/5/5.2 1030 Wien T +43 1 9741706 office@infraprotect.com www.infraprotect.com

UNTERNEHMEN	BESCHREIBUNG	KONTAKT/WEBSEITE
KAPSCH BUSINESSCOM	Kapsch BusinessCom ist als Digitalisierungspartner für Unternehmen tätig. Im Bereich der IT-Security bieten sie Lösungen in der Prävention von IT-Angriffen, der Network Protection durch Firewalls und Encryption sowie allgemeine Überwachungssoftware zur Erkennung von Unregelmäßigkeiten an. Ebenso werden eigene Workshops zur Fortbildung im Bereich der IT-Security angeboten. Auch ein eigener Report zum Thema Cyber Security wird mittlerweile publiziert.	Wienerbergstraße 53 1120 Wien T +43 508110 kbc.info@kapsch.net www.kapsch.net
KIWISECURITY SOFTWARE	KiwiSecurity ist ein führender Hersteller von Videoanalyse und Videoleitstellenlösungen, welche Videoüberwachung in ein proaktives Werkzeug wandeln. Durch die intelligente Auswertung relevanter Bildinformationen wird Videoüberwachung erstmals automatisiert.	Guglgasse 15 1110 Wien T +43 1 9971039 office@kiwisecurity.com www.kiwisecurity.com
KPMG AUSTRIA	KMPG bietet ein breitgefächertes Produktfeld in Bezug auf Cybersecurity auf. Sie führen beispielsweise Audits durch, um spezifische Risiken von IT-Systemen erfassen und bewerten zu könen, stellen individuelle Leitfäden zur Risikominimierung und Etablierung von Schutzmaßnahmen zur Verfügung und unterstützen Unternehmen ebenso bei akut auftretenden Cyberangriffen.	Porzellangasse 51 1090 Wien T +43 1 31332 home.kpmg/at/de/home/industries/technology.html
MAG MENTAL ACROBATICS GROUP™	MAG Mental Acrobatics Group bietet ein umfassendes Portfolio für IT-Security in Unternehmen an. Neben Dokumentationen, Audits und Schulungen werden eine Vielzahl unterschiedlicher Hard- und Softwarelösungen angeboten, die einen optimalen Schutz kritischer Netzwerke und Infrastrukturen gewährleisten können. Ebenso weist das Unternehmen Expertise im Bereich der Social Security und hinsichtlich rechtlicher Fragen (DSGVO) auf.	Arsenal Objekt 16 Top 66 1030 Wien T + 43 1 40600970 office@magsecurity.at www.magsecurity.at
PWC ÖSTERREICH	PwC unterstützt Unternehmen dabei sich optimal gegen digitale Bedrohungen zu schützen. Mit Experten auf den Gebieten der Informationssicherheit, Datenschutz, Digital Identity, IT-/OT-Security, Awareness und Business Continuity Management stellt PwC sicher, dass Unternehmen im Fall eines Cyberangriffs gewappnet sind. PwC schafft den Paradigmenwechsel bei den Mitarbeitern und integriert Cybersecurity als DNA in alle Geschäftsprozesse.	Donau-City-Straße 7 1220 Wien T +43 1 50188-0 cyber.austria@pwc.com Ansprechpartner: Georg Beham www.pwc.at/cyber

UNTERNEHMEN	BESCHREIBUNG	KONTAKT/WEBSEITE
RADAR CYBER SECURITY	Das Unternehmen Radar Cyber Security bietet Kunden umfassende Tools und Services für ihre Cybersecurity: IT und OT Security Monitoring, Advanced Cyber Threat Detection, IT und OT Risk Detection, Log Data Analytics (auch SIEM genannt) sowie CDC as a Service.	Zieglergasse 6 1070 Wien T +43 1 92912710 office@radarcs.com www.radarcs.com/de
REDPULS IT & SECURITY SOLUTIONS	redPuls IT & Security Solutions verfügt über ein speziell gefächertes Angebot im IT-Security Umfeld. Neben Next Generation Firewall, zählen hierzu auch Lösungen für Network-Web-Cloud-Ransomware Protection, DDoS Preventing, Mobile Device Security sowie allgemeine Penetration Tests und Networkmonitoring Tools. Zum organisatorischen Ablauf werden IT-Incident Management bzw. IT-Störungsmanagement Konzepte mit dem Kunden entwickelt und umgesetzt.	Neulinggasse 29/2/13 1030 Wien T +43 1 512 11220 office@redpuls.com www.redpuls.com
SBA RESEARCH	SBA Research ist ein COMET-Exzellenzzentrum für Informationssicherheit mit Standort Wien. In Zusammenarbeit mit u.a. TU Wien, sowie internationalen Institutionen, bietet ein dualer Ansatz aus wissenschaftlicher Forschung und praxisorientierter Umsetzung ein einzigartiges Leistungsangebot, das von Forschungskooperationen bis zu Penetrationstests reicht und Sicherheitsaspekte zukünftiger Schlüsselbereiche wie AI, IoT/Industrie 4.0, sichere Softwareentwicklung und Sicherheit in der Digitalisierung abdeckt. Ergänzt wird dies durch ein umfassendes Schulungsangebot.	Floragasse 7 1040 Wien T +43 1 5053688 office@sba-research.org www.sba-research.org
SEC CONSULT	SEC Consult ist professioneller Berater im Bereich Cyber- und Applikationssicherheit. Zum Portfolio zählen neben allgemeinen Sicherheitsüberprüfungen der IT-Systeme von Unternehmen und Behörden unter anderem auch Tätigkeiten im Prozessmanagement zur Gewährleistung gesetzlicher Vorgaben. Ebenso werden Lösungen zur Implementierung von Security-Maßnahmen bei der Softwareentwicklung angeboten.	Leopold-Ungar-Platz 2/3/3 1190 Wien T +43 1 89030430 office@sec-consult.com www.sec-consult.com

UNTERNEHMEN	BESCHREIBUNG	KONTAKT/WEBSEITE
SECURITECTS	Securitects ist professioneller Berater im Bereich IT- und Informationssicherheit. Sie unterstützen Unternehmen bei der Umsetzung der Norm ISO 27001 in Form von Sicherheitsrichtlinien, -prozessen und -verfahren. Securitects ist ebenso spezialisiert auf die Durchführung von Penetration Tests und IT-Forensik-Analysen. Dabei erhalten Unternehmen einen umfassenden Blick auf die Sicherheit ihrer IT-Systeme und klare Handlungsempfehlungen, dort wo Handlungsbedarf besteht. Persönliche Workshops und Trainings in den Bereichen ISO 27001 und sichere Software Entwicklung runden das Angebot ab.	Schelleingasse 8/9 1040 Wien T +43 1 9666471 office@securitects.com www.securitects.com/
SELECT-IT	SELECT-IT weist eine große Palette eigener Produktlösungen im Bereich der IT-Security auf. Dazu zählen beispielsweise Firewall- und Viren-Lösungen. Ebenso bieten sie Management & Monitoring an, sodass bei Problemen ein schnelles Eingreifen durch eine Fernüberwachung möglich ist. Auch für Bildungseinrichtungen ist das Unternehmen zum Thema IT-Security tätig.	Schuhfabrikgasse 17/3/4 1230 Wien T +43 1 36191010 office@select-it.at www.select-it.at/
SIEMENS ÖSTERREICH	Siemens setzt sich als großer internationaler Konzern auf verschiedenen Ebenen für eine Bewusstseinsschaffung von IT-Security ein. Neben einer Charter of Trust, die gemeinsam mit einer Vielzahl anderer Unternehem publiziert wurde, ist Siemens auch bei Veranstaltungen wie der Graz Security Week präsent.	Siemensstraße 90 1210 Wien T +43 1 517070 kontakt.at@siemens.com new.siemens.com/at/de.html
T3K-FORENSICS	T3k-Forensics ist als Service- und Schulungsberater für nationale und internationale Strafverfolgungsbehörden im Bereich der Mobilen Forensik tätig. Dazu zählen die Sicherstellung und Auswertung mobiler Geräte und Cloud-Daten, Forensische Trainings & Workshops mit Behörden im europäischen Raum sowie Lösungen im Mobile Security Bereich zur Erkennung und Abwehr von Bedrohungen bei mobilen Geräten.	Jacquingasse 51/3 1030 Wien T +43 1 9971033 office@t3k.ai www.t3k-forensics.com/de
TECHBOLD	techbold bietet als Unternehmen im Bereich der Cybersecurity ein große Palette an Produktlösungen an: Neben Audits, um den Ist-Zustand der Sicherheit von IT-Systemen zu bewerten, finden sich auch Firewalls, Datensicherungen und Anti-Spam Lösungen im Portfolio des Unternehmens.	Dresdner Straße 89 1200 Wien T +43 1 3434333 office@techbold.at www.techbold.at

UNTERNEHMEN	BESCHREIBUNG	KONTAKT/WEBSEITE
THALES AUSTRIA	Thales ist als internationals Unternehmen ein Global Player im Bereich der Cybersecurity. Sein Portfolio reicht von Datenverschlüsselung über Big Data Analysen und Threat Intelligence, wodurch jederzeit das Bedrohungspotenzial von Cyberangriffen bewerten werden kann, bis hin zu eigenen Cybersecurity Zentren, wo extern Bedrohungen in IT-Systemen von KundInnen in Echtzeit analysiert werden können und auf diese sofort reagiert werden kann.	Handelskai 92 1200 Wien T +43 1 277110 office.at@thalesgroup.com www.thalesgroup.com
T-SYSTEMS AUSTRIA	Als Großkundensparte der Deutschen Telekom unterstützt T-Systems bei der Planung und Implementierung maßgeschneiderter Security-Lösung wie Cyber Defence, Security Assessments, IP DDoS Security, Incident Response, SIaaS zum Schutz der IT-Infrastruktur, Managed Firewall Services für Unternehmen, sowie mit einem eigenen Security Operations Center (SOC) in Wien.	Rennweg 97–99 1030 Wien T +43 057 0570 security-info@t-systems.at www.t-systems.at
TECHNISCHE UNIVERSITÄT WIEN	Die TU Wien bietet innerhalb des Security-Bereichs folgende Schwerpunkte an: Kryptographie, Websicherheit, mobile Systeme sowie Anwendungen der Kryptographie für elektronische Währungen, Cloud- und Datenanalyse unter Bewahrung der Privatsphäre. Sie ist auch am International Secure Systems Lab (iseclab), einer Vereinigung von fünf internationalen System- und Sicherheitsforschungslaboratorien, beteiligt.	Karlsplatz 13 1040 Wien T +43 1 58801-0 pr@tuwien.ac.at www.tuwien.at
XSEC	Das Unternehmen XSec überprüft als Cybersecurity Unternehmen die Sicherheit von Unternehmen in unterschiedlichen Gebieten. Dabei werden auch die MitarbeiterInnen des Unternehmens selbst hinsichtlich ihrer Vorgehensweisen bewertet. Des Weiteren werden Trainings zum Bereich IT-Security und Beratungsgespräche mit Unternehmen, in denen zentrale Punkte im Bereich der IT-Security wie die Norm ISO 27001 erklärt werden. Ebenso kann XSec als externer Berater, beispielsweise im Bereich des Datenschutzes, angefordert werden.	Mayerhofgasse 6, 5. Stock 1040 Wien T +43 69910242048 bboeck@xsec.at Ansprechpartner: DI Mag. Mag. Benjamin Böck www.xsec.at

10. Impressum

Technologie Reports gibt es zu den Themen:

- Big Data und AI
- Cloud-Computing
- E-Government
- E-Health
- Enterprise Software
- Entertainment Computing
- IT Security
- FinTech
- Internet of Things
- E-Commerce
- Mobile Computing
- HR-Tech
- User Centered Design
- Visual Computing

Die digitalen Versionen finden Sie unter
www.wirtschaftsagentur.at/technologie/technologiestandort-wien/digitale-technologien/

Wirtschaftsagentur Wien.
Ein Fonds der Stadt Wien.
Mariahilfer Straße 20
1070 Wien
wirtschaftsagentur.at

Kontakt

Bernhard Schmid
Technologie Services
T +43 1 25200-521
schmid@wirtschaftsagentur.at

Text und redaktionelle Bearbeitung

eutema GmbH
Lindengasse 43/13
1070 Wien

Gestaltung

seitezwei.com

Fotos

Wirtschaftsagentur Wien/Karin Hackl,
Wirtschaftsagentur Wien/Klaus Vyhnalek

Die Informations- und Vernetzungsangebote werden im Rahmen des Projektes „IC3 Innovation by Co-Operation, Co-Creation and Community Building“ aus Mitteln des Europäischen Fonds für regionale Entwicklung kofinanziert.

Die Informations- und Vernetzungsangebote werden im Rahmen des Projektes „IC3 Innovation by Co-Operation, Co-Creation and Community Building“ aus Mitteln des Europäischen Fonds für regionale Entwicklung kofinanziert.

wirtschafts agentur wien

Für die Stadt Wien

Kontakt

Wirtschaftsagentur Wien.
Ein Fonds der Stadt Wien.
Mariahilfer Straße 20
1070 Wien
wirtschaftsagentur.at