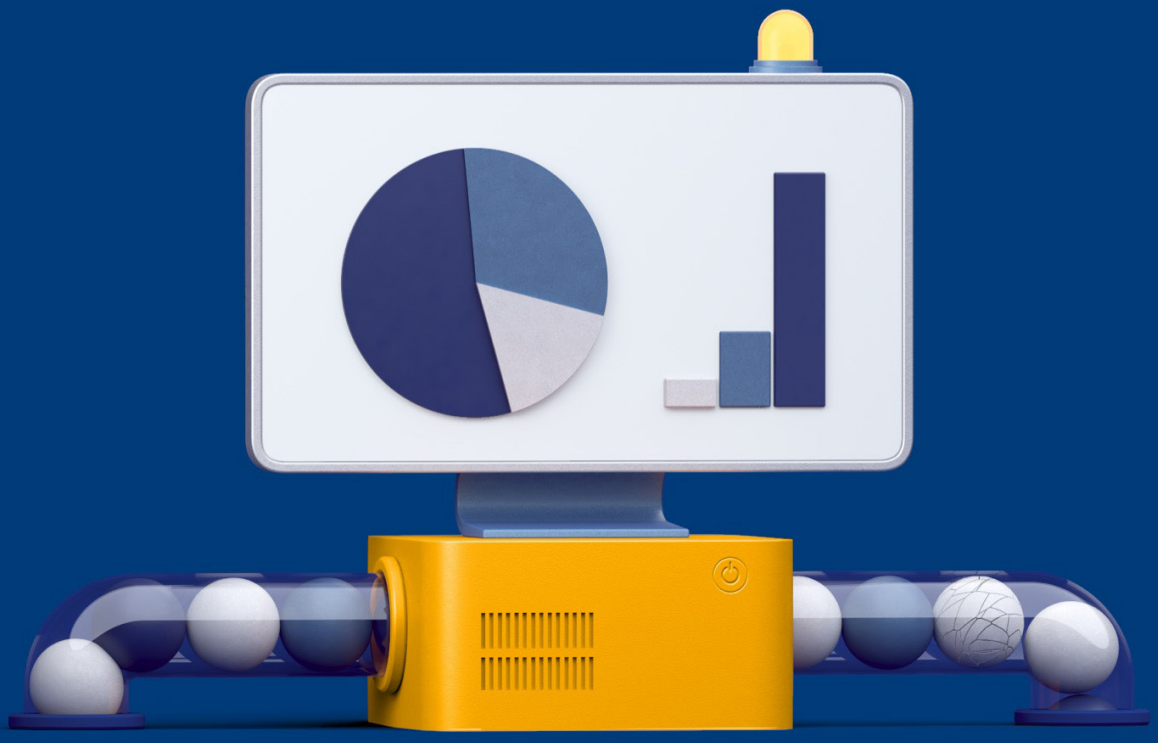
Emitec
IT-Management Report
2022 - Das Jahr der virtuellen Aufrüstung



emitec
datacom

Liebe LeserInnen

Auch dieses Jahr haben wir eine generelle Umfrage in verschiedenen IT Management Abteilungen durchgeführt. Wir richteten uns an Führungskräfte, die hauptsächlich mit der Planung, Strategie, Betreuung und Führung von IT-Firmen, -Abteilungen und – Projekten beauftragt sind.

Dabei spielen, wie bei jedem Unternehmen, personal- und finanzwirtschaftliche Kapazitäten eine tragende Rolle. Die von der Hälfte der Befragten tatsächlich als zu "gering" eingeschätzt wird (48 %). Eine leichte Mehrheit (52 %) findet, sie habe "ausreichend" Mittel, um ihre Ziele zu erreichen. Sind das die grössten Differenzen innerhalb der Branche?

Es sieht nicht so aus: Der Kampf gegen Cyber Security steht zuoberst auf der Prioritätsliste. Weil 2021 mit unzureichenden Sicherheits- und Personalstrukturen unautorisierte Zugriffe, Manipulationen oder sogar Diebstahl riskiert wurden.

Eine positive Tendenz ist erkennbar – kritische Infrastrukturen sind vielerorts wesentlich stabiler und die Service-Angebote breiter aufgestellt. Ausserdem wurden unter Hochdruck – Zeit wurde als wichtiger Sicherheitsfaktor erkannt – eine Armada an vielschichtigeren Security-Lösungen entwickelt und / oder installiert. Security Tools für E-Mail, Cloud Computing, AWS, OT und IT sind heute Standard.

Dennoch gibt es viel zu tun. Das zeigt unsere Studie auf, die eine wertvolle Entscheidungshilfe für business-kritische Entscheidungen sein kann. Gerade in Bezug auf Budgetplanung, Beschaffung, Prozessoptimierung sowie weitere Projekt- und MitarbeiterInnen-Entwicklung.

Ich wünsche Ihnen mit der informativen Lektüre viel Spass und weiterhin gutes Gelingen - für weitere Fragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Beste Grüsse

Stefan Betschart
Emitec Datacom

Inhaltsverzeichnis

1. Status Quo - Vadis?

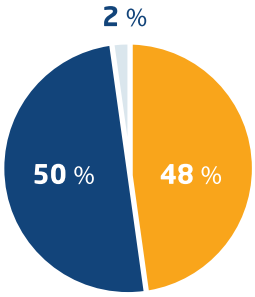
In der Studie, an der 129 IT-Entscheider und Leiter aus verschiedenen Unternehmen teilnahmen, legten alle ihren Fokus 2022 auf die Verbesserung von Cyber Security und die Effizienz-Steigerung der IT Services. Vor allem, weil man erkannt hat, bisher zu wenig personelle Ressourcen eingesetzt zu haben. Interessanter Fakt: Der hohe Anteil bisher eingesetzter Tools wirkt sich negativ auf die Effizienz aus.

Wie bringt man dies in Einklang mit der Erkenntnis, dass mangelnde Ressourcen und Know-How infolge stetig wachsender Komplexität herausfordernd sind? Einer der Ansätze ist, Prozesse vermehrt zu automatisieren.

Was ist den Befragten bei der Auswahl von Security-Lösungen wichtig? Technische Komplettheit, Funktionsumfang und Usability stehen ganz oben auf der Liste. Interessant ist, dass Kosten zwar auch ein wichtiger Faktor, aber nur ungefähr einem Viertel sehr wichtig sind.

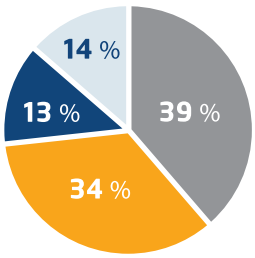
Sind diese personellen Ressourcen Ihrer Meinung nach

eher zu viel	0
ausreichend	62
eher zu wenig	64
keine Angabe	3



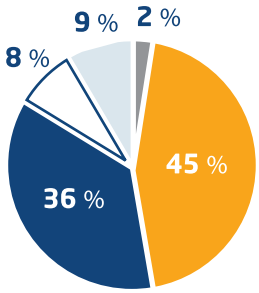
Wie hat sich das IT-Budget in Ihrem Unternehmen / Ihrer Abteilung im Vergleich zum letzten Jahr verändert?

Bleibt ungefähr	50
Wurde vergrössert	44
Wurde verkleinert	17
Weiss nicht / keine Angabe	18



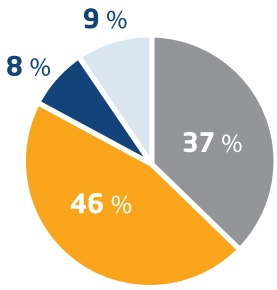
Wie viele Security / Management - Tools sind in Ihrem Unternehemen / Ihrer Abteilung aktuell im Einsatz?

Keines	3
1-5	58
5-15	47
15-30	10
30+	11

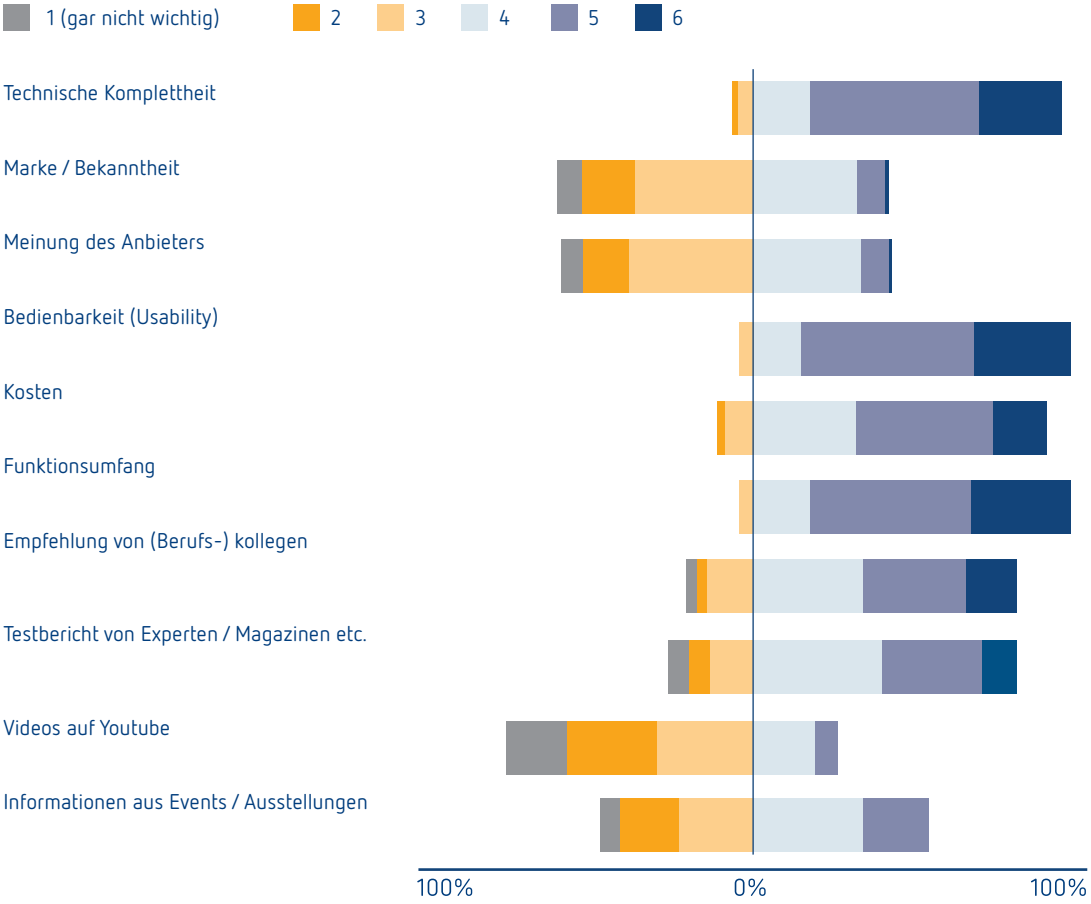


Die Anzahl der Tools ist im Vergleich zum Vorjahr...

Höher	48
Gleich gelblieben	59
Tiefer	10
Weiss nicht / keine Angabe	12



Geben Sie die Wichtigkeit der folgenden Punkte bei der Suche nach neuen Lösungen im IT-Umfeld in Schulnoten an



2. Basis unserer Befragung

Emitec AG hat 129 Teilnehmer aus verschiedenen Klein-, Mittel- und Gross-Unternehmen im Zeitraum von Februar bis März 2022 befragt.

Führende Entscheider aus der Telekommunikation (22 %), Dienstleistung (18 %), öffentlicher Verwaltung (12 %), Industrie (10 %), Finanzen (7 %), Verkehr / Tourismus / Gesundheit (je 5 %) und 16 % andere Branchen.

Die meisten, 66 %, waren Mitarbeiter von Firmen mit bis zu 5000 Mitarbeitern, 34 % aus Unternehmen mit deutlich mehr Beschäftigten.

78 % kommen aus dem IT Management, 51 % sind für IT Security zuständig und 29 % arbeiten in beiden Bereichen. 60 % in einer Kaderfunktion.

3. Wer macht was?

101 der Befragten sind im IT Management angesiedelt – gemäss unserer Studie. Und wie bewerten sie ihr Arbeitsumfeld bzw. die Qualität ihrer IT Services? 88 % befinden die Situation als gut - mit Optimierungspotenzial. Nur 6 % sehen starken Handlungsbedarf. Ebenso viele sind "sehr gut" von ihrem IT Management überzeugt.

4. Wie gut sind wir?

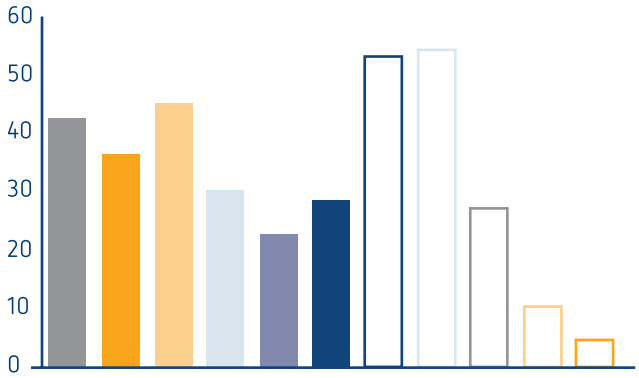
Wir wollten von den Probanden wissen, wie sich selber einschätzen. Welche Schulnoten würden sie sich geben, wenn sie ehrlich beurteilen. Ohne zu schummeln und den Nachbarn zu fragen. Praktisch die Hälfte der Befragten antwortet mit "Ich bin gut bis sehr gut", geben sich eine 5,5 - was erfreulich ist. Denn ein gutes Selbstbewusstsein im Einklang mit Kompetenz ist für eine erfolgreiche Performance eminent wichtig. Besorgniserregend ist eher, dass starke 39 Prozent sich "genügend", also eine 4, geben. Finden also, ihre Fähigkeiten seien ausbaufähig. Sogar 12 Prozent finden, sie können zu wenig, benoten sich mit "ungenügend" - eine glatte 3! Hier muss man ansetzen und das Know-How und den Wohlfühlfaktor der MitarbeiterInnen dringend regelmässig überprüfen. Ein Unternehmen ist nur so gut, oder in diesem Fall so "sicher" wie seine MitarbeiterInnen.

5. What's hot this year?

Die meisten der Befragten planen in den nächsten 12 Monaten Projekte Service- und Infrastruktur-Optimierungs-Management, dicht gefolgt von Network Performance & Analyse. Auch Verbindungs- und Netzwerk-Qualität ist ein grosses Thema.

In welchen der folgenden IT-Management-Themen sind in Ihrem Unternehmen in den nächsten 12 Monaten Projekte geplant?

Automation & Software Robotic	42
Service & Applikationen testen	36
Verbindungs- und Netzwerkqualität	45
Performance und Load Tests	30
IT-Service & AIOps Monitoring	22
Enduser-Experience überwachen	28
Network Performance & Analyse	53
Infrastruktur Management	54
Intelligente Datensammlung	27
weiss nicht / keines der genannten	10
Sonstiges	4



6. Wie gut sind wir besetzt?

Von den Befragten gaben 51% an, effektiv im Bereich IT-Security tätig zu sein, obwohl sie mindestens eine sicherheitskritische Schnittstelle haben, wenn sie im IT Management arbeiten. Hier besteht ein Zusammenhang mit der klaren Ausbildung von Angestellten und verschärfter Awareness für IT Security im Allgemeinen.

Sind sie im Bereich IT-Security tätig?

Ja	66
Nein	63

7. Wieviel Luft nach oben haben wir?

Auch hier liessen wir leitende bzw. Entscheidende Angestellte den allgemeinen Output ihrer Arbeit benoten. Denn 82 % der befragten Entscheider und Abteilungsleiter benoten ihre IT Security als "genügend mit Optimierungspotenzial" - das gibt eine 4 +. Damit kommt man nicht auf die nächste Stufe, sondern wird von den Klassenbesten abgehängt. Es gibt also Room To Improve – und dieses Verbesserungspotenzial muss ausgeleuchtet werden. So schnell wie möglich. Nur 6 % geben ihrem Sicherheitssystem die Bestnote "Sehr gut", schreiben eine 6. Die dürfen ihre Sachen packen und frei machen – 94 % müssen nachsitzen.

8. Was wissen wir schon?

Wie benoten die Probanden ihr eigenes IT-Security-Know-How? Hier schreiben gute 47 % eine 5,5 bis 6 – die Bestnoten. Dass aber auch hier 39 % sich gerade mal mit einer mageren 4 durchschlagen, ist "genügend", aber in Bezug auf das allgemeine IT-Sicherheitswohlbefinden "unbefriedigend". Gerade, wenn sogar 14 %, die tagtäglich in mit diesen kritischen Themen zu tun haben und verantwortlich sind, sich eine 3 geben - "ungenügend". Wir sehen also, dass Unternehmen mehr Klassenbeste ausbilden müssen.

9. Awareness, Annahme, Attacke

Die Tendenz geht klar Richtung: Fortlaufende Weiterentwicklung der IT-Infrastruktur. Personell, aber auch technologisch jederzeit die lückenlose Funktionssicherheit gewährleisten.

Mit stets wachsamem "real time" Auge und smarter Weiterentwicklung von effektiven Tools und Prozessen für einen 24/7-Schutz vor Bedrohungen aus aller Welt. Letzteres ist Fakt, und wir müssen uns als Teil der lokalen Lösung eines globalen Problems sehen. Dafür ist es wichtig, Awareness zu schärfen und die Situation anzunehmen. Dann entsprechende Massnahmen treffen, Prozesse optimieren, MitarbeiterInnen weiterentwickeln – und auf IT Security einschwören.

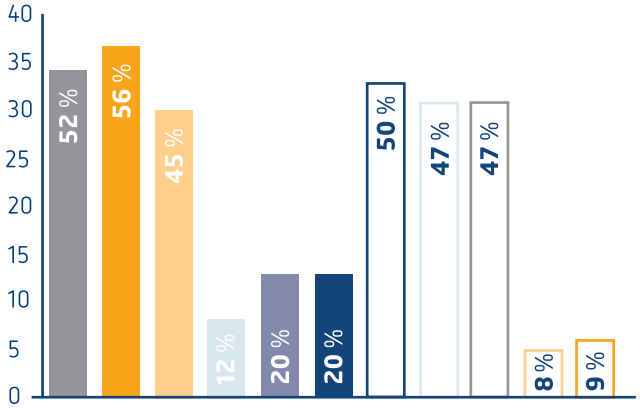
Aktuell haben wir Schweizer noch Luft nach oben: Im Global Security Index belegen wir den bequemen Platz 42. Das können wir besser. Indem wir die erarbeiteten Erkenntnisse clever und entschieden in zielführende Lösungen einfliessen lassen.

Eigentlich simpel: Skills, Personal, Performance, Prozesse und Tools regelmässig auf die Entwicklung der weltweiten Bedrohungslage prüfen - und sichern.

Das geschieht gerade über einen enormen Anstieg von Testing und Monitoring, mit Schwerpunkt Detection, Cloud Response, Netzwerk und Endpoints. Und immer mehr IT-Manager setzen auf Real Time Visibility, konstante Vulnerability Scans und Angriffssimulationen.

In welchen der folgenden Security-Themen sind in Ihrem Unternehmen in den nächsten 12 Monaten Projekte geplant?

Risk-Assessment	34
Vulnerability-Scan	37
Angriffs-Simulation	30
Securuty Limit Tests	8
DDoS & Edge Defense	13
XDR (Next gen. SIEM)	13
Endpunkt-Sicherheit (EDR)	33
Netzwerk-Sicherheit (NDR, NTA)	31
Cloud-Sicherheit	30
weiss nicht / keines der genan...	5
Sonstiges	6



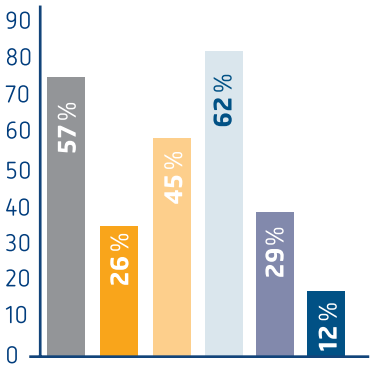
Der Hauptfokus liegt allgemein auf Verbesserung von Cyber Security, Erweiterung von IT Services Installationen und Steigerung der Anwenderzufriedenheit. Natürlich ist auch Effizienzoptimierung oben auf der Agenda und löst Usability und Kostenreduzierung ab, die als Themen nur einem Viertel der Befragten noch relevant scheinen.

Ein gutes Zeichen: Die Budgetbremse wird allgemein gelockert und auf Bequemlichkeit verzichtet, zu Gunsten von Ausbau, Sicherheitsoptimierung und Effektivität der priorisierten Massnahmen. Der Angriffsmodus ist an.

2022 – im Jahr der virtuellen Aufrüstung.

Was ist der Hauptfocus in der IT Ihres Unternehmens / Ihrer Abteilung in den nächsten Monaten?

Erhöhung der Effizienz	74
Reduzierung der Kosten	34
Erweiterung oder Einführung neuer IT Services	58
Verbesserung der Cybersicherheit	81
Steigerung der Anwenderzufriedenheit	38
Sonstiges	16



Testen. Monitoren. Optimieren.

Die erfolgreiche Emitec-Strategie

Emitec AG, Birkenstrasse 47, CH-6343 Rotkreuz, T +41 41 748 60 10
www.emitec-datacom.ch, info@emitec.ch