Confare: Creative. Innovation. Session.

in Kooperation mit Check Point SOFTWARE TECHNOLOGIES LTD.

Factsheet

IT-Security Agenda für das Digitale Zeitalter

www.confare.at

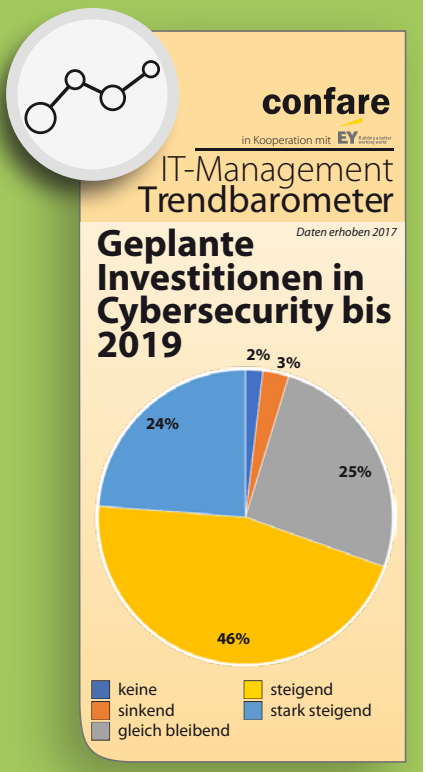
In einer Welt der zunehmenden Vernetzung und digitalisierten Wirtschaft ist der sichere Umgang mit Daten entscheidend, um die Wertschöpfung gewährleisten zu können. Informationstechnologie ohne den Aspekt der IT Sicherheit miteinzubeziehen ist undenkbar. Datenbasierte Produkte können nur dann funktionieren, wenn der sichere Umgang mit den Daten umfassend und rechtzeitig berücksichtigt wird. Doch welche Erfolgsfaktoren müssen für einen effektiven Schutz ihres Unternehmens berücksichtigt werden?

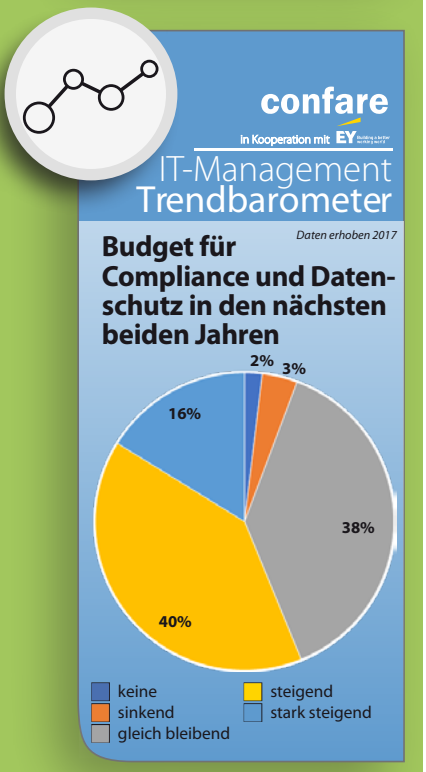
Im Rahmen einer Confare Creative Innovation Session haben IT-Manager gemeinsam mit den Experten von Check Point Software Technologies eine Roadmap erarbeitet, die alle wichtigen Bausteine aufzeigt, damit Cybersecurity Innovation möglich machen kann anstatt sie zu verhindern.

Die CIS wurde geleitet von Philipp Slaby, Check Point Software Technologies und Walter Hölblinger, CIO von Steyr Mannlicher.

9 Bausteine, die Ihre IT-Security Agenda zukunftsfähig machen

1. **Awareness ist der Schlüssel für eine zukunftsfähige IT-Security Strategie**
   Technologie alleine macht Ihre IT nicht sicher. In immer ausgefeilteren Attacken werden Mitarbeiter zum Hauptangriffsziel der Bösewichte. Schärfen Sie das Bewusstsein Ihrer Mitarbeiter für IT-Security. Durch **innovative und kreative User-Awareness Trainings** verschaffen Sie Ihren Anwendern Verständnis über alle relevanten Maßnahmen.
2. **Quantifizieren Sie nicht nur die Kosten, sondern auch den Nutzen von IT Sicherheitsmaßnahmen**
   Security ist eigentlich immer nur unangenehm. Sie macht weder Spaß noch trägt sie offensichtlich zum Gewinn bei. Doch gerade bei Digitalen Innovationen ist Security ein Faktor der Wertschöpfung. Wer mit Daten sicher umgehen kann, kann mit Daten auch Geld verdienen. Wenn Sie Geschäftsführer mit einbinden und den Vorstand sensibilisieren, sind die Kosten für IT-Security nur mehr zweitrangig. Sie diskutieren dann über Wert und nicht über Einsparungen.
3. **Schaffen Sie Transparenz und zeigen Sie Erfolge auf**
   „Tue Gutes und rede darüber" gilt nicht nur im Marketing. Wie Sie mit Risiko umgehen und Gefahren abwehren, schafft nicht nur mehr Akzeptanz, sondern sorgt auch dafür, dass die Mitarbeiter im Unternehmen Security ernst nehmen.
4. **Reduktion der Komplexität**
   Für den User sollten die Sicherheitslösungen soweit möglich „unsichtbar im Hintergrund" arbeiten. Dabei steht stets die Benutzerfreundlichkeit, die hohe Usability im Vordergrund. Um die Komplexität von IT-Security für die User zu minimieren, müssen Sie **Transparenz der internen Workflows** schaffen. Klarheit über die Funktion und das Z**usammenspiel der IT Applikationen** sind eine Grundvoraussetzung, um IT Sicherheitsmaßnahmen erfolgreich implementieren zu können.





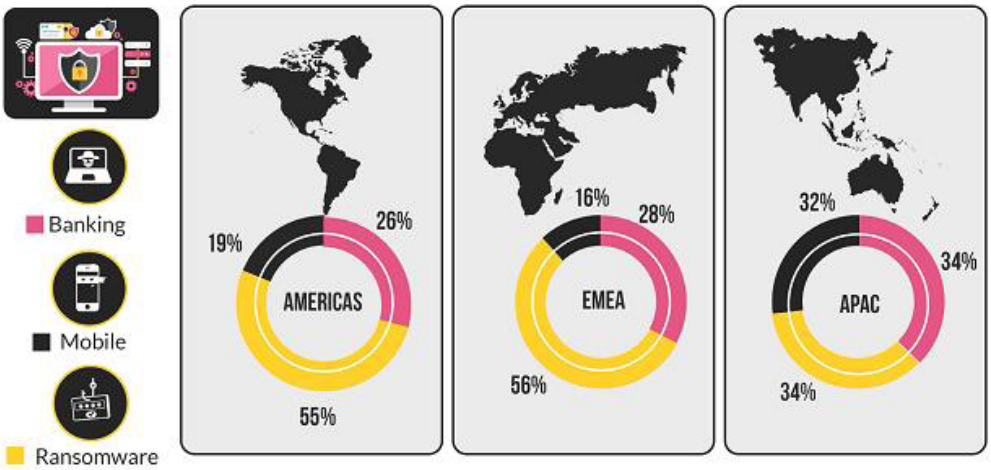
5. **Must Have oder Hype? Messen Sie das Risiko von Technologie-Entscheidungen**
Noch nie gab es so viele junge Technologieunternehmen mit innovativen Produkten. Viele davon könnten auch in Ihrem Unternehmen nutzbringend eingesetzt werden. Andere sind Zeitverschwendung und werden sich nicht durchsetzen und auch nicht den entscheidenden Vorteil bringen. Eine Risikobewertung hilft, Prioritäten zu setzen und zukunftsorientierte Technologieentscheidungen zu treffen. Voraussetzung für einen effektiven Mehrwert in Ihrem Unternehmen ist das **Zusammenspiel mit bestehenden Schutztechnologien**. Die **Komplexität aktueller Angriffe** setzt voraus, dass Auffälligkeiten bzw. Abweichungen vom Regelzustand auf allen Ebenen erkannt und in einem **konsolidierten System** dargestellt werden können.

6. **Schaffen Sie eine ganzheitliche Sicht auf die Bedrohungslage**
Technologie ist kein Selbstläufer (keine Checkbox). Maßnahmen zur Präventation von Angriffen sind essentiell, stellen aber nur einen Teil der gesamten IT Sicherheit dar. Um Cyber-Attacken schnellstmöglich zu entdecken, den Schaden zu begrenzen und die Ursache beseitigen zu können, werden neben den **Präventationstechnologien** auch Instrumente zur **Erkennung** und **Reaktion** notwendig. Darüber hinaus sollten innovative Lösungen eingesetzt werden, welche das **Darkweb analysieren**, um bereits vor dem tatsächlichen Angriff Unternehmen proaktiv informieren zu können.

7. **Security as a Service macht Ihr Schutzschild flexibel**
Neue Geschäftsmodelle und Verrechnungssysteme bieten dem Kunden neue Möglichkeiten. „Pay as you go"-Modelle können flexibel und agil auf Veränderungen angepasst werden und ermöglichen es Ihnen, neue Produkte, Services und Innovationen schnell und kosteneffizient umzusetzen und dabei den Security Level aufrecht zu erhalten.

8. **Integrieren Sie Sicherheit von Beginn an in Prozesse und Projekte**
Sie führen ein neues System ein und erst am Ende kommen auch Security Überlegungen ins Spiel? Dann sind die Kosten hoch und das Ergebnis nicht zufriedenstellend. Wenn Sie von Beginn an die Aspekte der Cybersecurity berücksichtigen, kommen Sie weiter. Dann können dabei sogar neue Ideen stehen und neuer Wert geschaffen werden.

9. **DSGVO und Compliance – Wenn Sie glauben Security ist teuer, probieren Sie es mal ohne ….**
IT-Sicherheit ist ein wichtiger Faktor, um die rechtlichen Rahmenbedingungen zu erfüllen. So können Sie Innovation und Compliance gemeinsam sicherstellen.



Ihr Ansprechpartner:

Philipp Slaby, MSc

Security Consultant bei **Check Point Software Technologies GmbH**
pslaby@checkpoint.com | tel. +43 1 99 460 6701 | www.checkpoint.com

Check Point SOFTWARE TECHNOLOGIES LTD.

Im Confare-Blog:

Innovative CIO - 7 steps to creativity and business innovation in your IT department

7 Steps to become an Innovative CIO – How IT Leaders Can Drive Business Transformation Created in cooperation with EY Switzerland and the Confare CIO Advisory Board.
www.confare.at/innovative-cio-7-steps-creativity-business-innovation-department/