EVIDEN
an atos business

Cybersecurity

Geschützt in die Zukunft

Die Herausforderung

Die rasante Geschwindigkeit der digitalen Transformation stellen Wirtschaft und Gesellschaft vor neue Herausforderungen. Die Bedrohungslandschaft wird komplexer, die Wirtschaft digitaler. Moderne Kommunikationssysteme, Milliarden IoT-Devices (Geräte im Internet der Dinge) für Lieferketten, Smart City und Smart Manufacturing sind nur einige Beispiele für eine deutlich vergrößerte Angriffsfläche für Cyberattacken. Auch viele Bereiche des alltäglichen Lebens werden in die digitale Welt verlagert. Mit der Stärkung von Home-Office und dezentralen Arbeiten im Rahmen der Coronapandemie wurden weitere Angriffspunkte geschaffen. Teils ungesicherte digitale Infrastrukturen und Endgeräte stellen ein erhebliches Sicherheitsrisiko dar.

Schon vor der Coronapandemie entstand in der deutschen Wirtschaft durch Cyberangriffe ein jährlicher Schaden von mehr als 100 Milliarden Euro. Im Durchschnitt werden drei von vier Unternehmen Opfer von Sabotage, Datendiebstahl oder Spionage. Die Liste der abschreckenden Beispiele ist lang. So verursachte die Schadsoftware Emotet seit dem ersten Auftreten im Jahr 2014 allein in Deutschland rund 14,5 Millionen Euro Schaden. Cyber-Erpressung kann sogar gut etablierte deutsche Mittelständler mit einem Milliarden-Umsatz wie Symrise, aber auch Organe der Rechtsprechung wie das Berliner Kammergericht stilllegen.

Neben Unternehmen sind auch Behörden und politische Organe, Einzelpersonen und zunehmend auch Betreiber kritischer Infrastrukturen betroffen und werden Opfer gezielter Angriffe. Selbst das „*Peleton*“-Trainingsrad des US-Präsidenten Joe Biden stellt durch seine Konnektivität zum Internet ein potenzielles Sicherheitsrisiko im Weißen Haus dar. In Reaktion auf die Krise ist auch in Deutschland die Arbeit der Parteien digitaler geworden. Virtuell durchgeführte Parteitage erfahren massive Cyberattacken. So rückt das Thema Cybersicherheit verstärkt in den Fokus politischer Entscheidungsträger.

Unser Ansatz

Als europäischer Marktführer und weltweite Nummer 3 im Bereich der Cybersicherheit ist sich Eviden der wachsenden Herausforderungen bewusst. Das Unternehmen leistet schon heute einen wichtigen Beitrag für den Schutz der europäischen Wirtschaft. Eviden ist in Deutschland vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als IT-Sicherheitsdienstleister zertifiziert.

Das Unternehmen ist überzeugt, dass Daten in Kombination mit menschlicher Intelligenz und Wissen der Schlüssel zur Bekämpfung heutiger Bedrohungen sind. Automatisierung und Maschinelles Lernen ermöglichen es, Risiken zu verstehen und Angriffe vorherzusagen. Preisgekrönte Innovationen wie *Alsaac* setzen Zukunftstechnologien wie Künstliche Intelligenz und Edge Computing zu ebendiesem Zweck ein. Zudem baut Eviden ausdrücklich auf die Kooperation mit kleinen und mittelständischen Unternehmen. So wird gewährleistet, dass die angebotenen digitalen Lösungen die entsprechenden Bedürfnisse nach Cybersicherheit

EVIDEN
an atos business

erfüllen. Denn sie sind das Rückgrat der deutschen und europäischen Wirtschaft und dadurch besonders schützenswert. Im Rahmen des Programms Eviden *Scaler* werden die Technologie-Teams von Eviden mit ausgewählten Start-ups zusammengebracht. Der Fokus liegt hier auf Sicherheit und Dekarbonisierung.

Im Bereich der Cybersicherheit arbeitet Eviden mit dem Operation Technology-Spezialisten „*Claroty*" zusammen. Ziel ist, die Verfügbarkeit, Sicherheit und Zuverlässigkeit von Betriebsanlagen und -netzwerken in Industrieunternehmen und kritischen Infrastrukturen zu verbessern.

Seit 2002 ist Eviden zudem Partner des Internationalen Olympischen Komitees (IOC) und verantwortet damit alle zwei Jahre den sicheren und reibungslosen technischen Ablauf der Sommer- und Winterspiele. Die Olympischen Spiele sind ein hochkarätiges Ziel für Cyberkriminelle, Hackerangriffe und Terroristen. Eviden hat daher eine Reihe von präventiven Cybersicherheitsdiensten und -lösungen entwickelt und implementiert, die das IOC vor Angriffen schützt.

Wir dürfen uns nicht damit abfinden, dass Cyberkriminelle uns immer ein Schritt voraus sind. Deswegen bereitet sich Eviden stets auf die **nächsten digitalen Schockwellen** vor – nicht zuletzt auf die Ankunft des Quantencomputers. Da die Angriffsfläche immer größer wird, ist Cybersicherheit nicht mehr nur eine Aufgabe für die IT-Abteilung. Es ist eine Führungsaufgabe, politische Führung inbegriffen. Eviden möchte sich in die Gestaltung der politischen Rahmenbedingungen konstruktiv einbringen und mit Expertise und Erfahrung als vertrauenswürdiger Partner an der öffentlichen Diskussion teilnehmen.

Unsere Positionen

Forschung und Investitionen in Cybersicherheit: Neue Techniken der Datenverschlüsselung, der Einsatz von Blockchain und ähnlichen Lösungen, digitale Forensik-Technologien, Angriffserkennung, künstliche Intelligenz und Quantencomputing spielen im Kampf um die Aufrechterhaltung der Widerstandsfähigkeit und Integrität von digitalen Netzwerken eine wichtige Rolle. Etwa 85 Prozent aller Cyberangriffe könnten mit dem richtigen Schutz verhindert werden. Daher gilt es, die Erforschung und die Entwicklung von Cybersicherheits-Lösungen zu intensivieren und zu priorisieren.

Sensibilisierung in Politik und Gesellschaft: Viele Cyberangriffe werden durch leichtsinniges Agieren der Nutzer, etwa dem Verschieben von Sicherheitsupdates, dem Öffnen von E-Mails mit gefährlichen Inhalten oder Nutzen eines unsicheren Passwortes erst ermöglicht. Das Befolgen einfacher Guidelines und Verhaltensregeln kann hier bereits Abhilfe schaffen. Ein kontinuierlicher und intensivierter Informationsfluss, nicht nur über die Notwendigkeit, in sichere digitale Lösungen zu investieren, sondern auch über die Unverzichtbarkeit eigenes Fehlverhalten vorzubeugen, ist von elementarer Bedeutung.

Innovative **Ende-zu-Ende-Cybersicherheit** wäre ein Wettbewerbsvorteil für Europa, der regulatorische Unterstützung braucht. Industrie-Initiativen wie der *Charter of Trust* fördern das Bewusstsein für Cybersicherheit und stärken das Vertrauen der Verbraucher in der digitalen Welt. Ihre Prinzipien wie Security by Default, Verantwortung in der gesamten digitalen Lieferkette und Transparenz muss sich auch in Cybersicherheits-Regeln wiederfinden.

EVIDEN
an atos business

Europäische Zusammenarbeit im Bereich der Cybersicherheit stärken: Cyberangriffe gehen über Nationalstaatsgrenzen hinaus und betreffen alle Mitgliedsstaaten der Europäischen Union. Eine enge Kollaboration und Förderung technologischer und digitaler Souveränität im Bereich der Cybersicherheit sind von großer Bedeutung.

Wirtschaftliche Anreize für Unternehmen setzen: Eine Umstellung in neue, sichere Cybersicherheitslösungen kann für viele, gerade kleine und mittelständische Betriebe, eine große finanzielle und personelle Belastung darstellen. Vom verbesserten Schutz dieser Unternehmen und der damit einhergehenden Reduzierung von Cybersicherheitsrisiken profitieren alle. Insbesondere im Bereich der kritischen Infrastrukturen ist dieser Ansatz wichtig. Ziel ist es, die deutsche Wirtschaft von einem reaktiven Cybersicherheitsansatz zu einem aktiven Ansatz zu verändern, denn nur so lässt sich auf die wandelnden Cybersicherheitsanforderungen angemessen reagieren.

Schwachstellen in der IT-Infrastruktur öffentlicher Behörden und Institutionen effizient schließen: Kommt es zu einem Hackerangriff auf eine politische Institution oder Behörde, ist der Schaden bereits angerichtet. Hier gilt es, aktiv für mehr Schutz zu sorgen und Lücken in der IT-Sicherheit zu schließen, bevor diese ausgenutzt werden können. Eine stetige Digitalisierung der öffentlichen Verwaltung muss in jedem Fall mit einer robusten Cybersicherheitsarchitektur einhergehen.

Dem **Fachkräftemangel im Bereich Cybersicherheit** entgegenwirken: Auch die besten Cybersicherheitslösungen können nur dann etwas bewirken, wenn es spezialisierte IT-Fachkräfte gibt, welche mit Anwendung und Wartung vertraut sind. Sowohl eine aktive Nachwuchs- und Talentförderung als auch eine qualifizierte Einwanderungspolitik für Fachkräfte können hier Lösungsansätze sein. Aktuell fehlen weltweit etwa 1,8 Millionen Cybersicherheitsexperten. Eviden selbst beschäftigt weltweit bereits mehr als 5000 Cybersicherheitskräfte, welche stündlich 125 Millionen Angriffe managen. Der Bedarf steigt kontinuierlich an.

Über Eviden

Eviden ist ein führendes deutsch-französisches Unternehmen in den Bereichen digitale Transformation, Big Data und Cybersicherheit, das in wachstumsstarken Märkten positioniert ist. Mit den zur Verfügung stehenden internen Synergiemöglichkeit will das Unternehmen in den kommenden Jahren sein Wachstum beschleunigen, indem es seinen Kunden höchst ausdifferenzierte Lösungen anbietet.

Eviden ist der weltweit führende Anbieter von Cybersicherheitsdienstleistungen und Europas einziger Hersteller von Supercomputern. Das Unternehmen bietet ein hochmodernes, souveränes Cloud-Angebot und verfügt über ein großes Fachwissen im Bereich der Anwendungsmodernisierung und -migration sowie über ein aufstrebendes Geschäft im Bereich der End-to-End Cloud Transformation. Eviden ist der europäische Partner für Umsetzung digitaler Souveränität durch digitale Unabhängigkeit, Datenschutz und die Sicherheit digitaler Räume.

EVIDEN
an atos business

Kontakt

Catherine Briat
SVP – Global Chief Sustainability Officer - Head of Public Affairs Germany
T: +4916097569039
M: +33766246188
E: catherine.briat@eviden.com