



KASPERSKY LAB:

UNSER ANSATZ FÜR DIE

INDUSTRIELLE IT-SICHERHEIT

Als eines der weltweit führenden Unternehmen im Bereich der Sicherheit für Unternehmen nimmt Kaspersky Lab auch bei der industriellen Sicherheit eine Vorreiterrolle ein.

DIE VORREITERROLLE VON KASPERSKY LAB

KASPERSKY LAB: SOLIDE SICHERHEIT UND IDEENFÜHRERSCHAFT.

Als weltweit größtes Privatunternehmen für IT-Sicherheit betreut Kaspersky Lab 300 Millionen Benutzer in 200 Ländern und Regionen rund um den Globus. Zum Kundenportfolio von Kaspersky Lab zählen über 250.000 Unternehmen weltweit – von kleinen und mittelgroßen Organisationen bis hin zu großen staatlichen Behörden und Wirtschaftsunternehmen. Mehr als 300 Millionen Menschen weltweit werden durch die Produkte und Technologien von Kaspersky Lab geschützt.

Unter der Führung unseres Gründers und Firmenchefs Eugene Kaspersky, einem weltweit anerkannten Experten und Visionär im Bereich Cybersicherheit, hat das Unternehmen sich einen Namen für ein wegweisendes Verständnis von lokalen und globalen Bedrohungen gemacht. Kaspersky Lab hat in den letzten Jahren viele der relevanten Sicherheitsvorfälle zuerst entdeckt, z. B. Dark Hotel, Flame, Gauss, mini-flame, Red October, NetTraveler und The Mask. Auch gezielte Angriffe auf industrielle Netzwerke wie Crouching Yeti (Energetic Bear) und Black Energy 2 wurden von Kaspersky Lab entdeckt.

IDEENFÜHRERSCHAFT BEI DER BEDROHUNGSANALYSE

Das Kaspersky Security Network ist eine komplexe, verteilte Infrastruktur, die auf den Echtzeitinformationen von über 60 Millionen freiwilliger Kaspersky-Kunden aufbaut. Gleichzeitig analysiert unser «Global Research and Analysis Team (GReAT) weltweit die aktuelle Bedrohungslage und entwickelt Lösungen zum Schutz vor der immer raffinierter werdenden Malware.

VORREITERROLLE BEI FORSCHUNG UND INNOVATION

Als privates Unternehmen sind wir in der Lage, große Investitionen in unsere Forschung und Entwicklung zu tätigen. Nahezu die Hälfte unserer weltweit 3000 Mitarbeiter sind in unseren Forschungs- und Entwicklungseinrichtungen tätig und beschäftigen sich primär mit der Entwicklung innovativer Technologien und der Analyse von Cyber-Kriegsführung, -Spionage und -Sabotage sowie allen Arten von Bedrohungen und Techniken.

Diese Fokussierung auf eine hochwertige, interne Forschung und Entwicklung hat Kaspersky Lab zu einem der Branchenführer im Bereich IT-Sicherheitstechnologien gemacht. Dies schlägt sich auch in den Bewertungen von unabhängigen Testlabors nieder, von denen wir mehr Top-Bewertungen erhalten als die meisten anderen Anbieter.

VERLÄSSLICHER PARTNER VON REGIERUNGEN UND BEHÖRDEN

Die Bedrohungsforschung war schon immer ein zentraler Bestandteil unserer Sicherheitsstrategie. Dank des weltweiten Teams aus anerkannten Experten und Analysten wurde Kaspersky Lab von der globalen IT Security Community zu einer fortlaufenden Kooperation und Beratungstätigkeit eingeladen. Zu dieser Community zählen u.a. auch Interpol, Europol, die Microsoft Digital Crimes Unit, IT-Sicherheitsagenturen sowie eine Vielzahl von CERTs und die ISA (International Society of Automation). Wir kooperieren derzeit eng mit den Behörden in einer Reihe von Ländern – von Russland bis hin zu den USA –, um zusammen die Rahmenbedingungen für den Schutz von Industrieanlagen und wichtigen Infrastruktureinrichtungen auszuarbeiten.

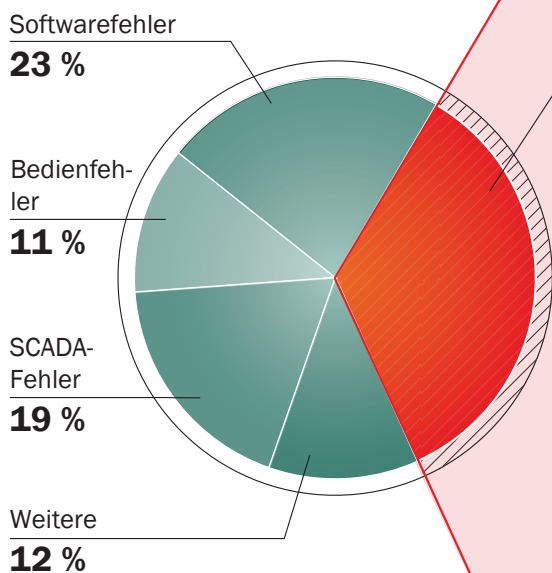
► UNSERE LAGEBEWERTUNG DER INDUSTRIELLEN SICHERHEIT

SIE MÜSSEN NICHT DAS ZIEL SEIN, UM ZUM OPFER ZU WERDEN. DESHALB FUNKTIONIERT DER DERZEITIGE ANSATZ ZUR INDUSTRIELLEN SICHERHEIT NICHT.

Bei einer aktuellen Umfrage des SANS Institute waren sich nur 9 % der befragten IT-Experten aus dem industriellen Sektor sicher, dass es in ihrem Unternehmen keine Sicherheitsverletzung gegeben hat¹. Bemerkenswerterweise gaben 16 % von ihnen an, dass sie über kein Verfahren zum Aufspüren von Schwachstellen verfügen, teilweise aus der Angst heraus, dadurch ungewollt Aufmerksamkeit auf diese Schwachstellen zu lenken.

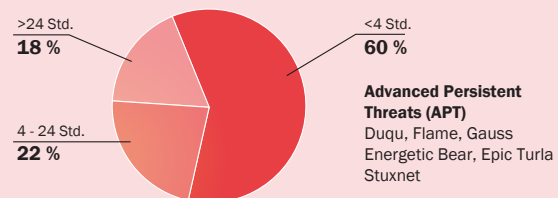
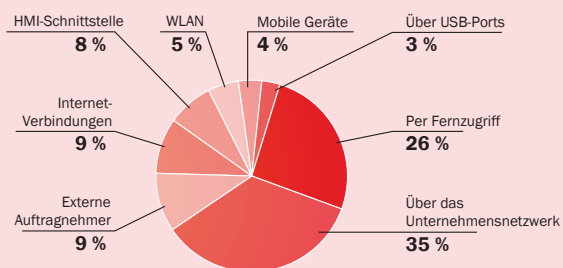
Aber Sie müssen nicht das Ziel sein, um zum Opfer zu werden. Zusätzlich zu den hochentwickelten Bedrohungen, die sich speziell gegen industrielle Anlagen richten, z. B. Citadel, Crouching Yeti/Havex, Miancha oder Black Energy 2, liegt eine weitere Gefahr in den alltäglichen Bedrohungen, die sich gegen den Teil Ihrer Infrastruktur richtet, in dem der normale Geschäftsbetrieb stattfindet.

BEDROHUNGEN: SIE MÜSSEN NICHT DAS ZIEL SEIN, UM ZUM OPFER ZU WERDEN



Hauptgründe für Ausfälle in industriellen Netzwerken
securityincidents.net

Malware-Angriffe 35 %



Advanced Persistent Threats (APT)
Duqu, Flame, Gauss
Energetic Bear, Epic Turla
Stuxnet

Allgemeine Malware
Viele ICS-Bedrohungen sind nicht sonderlich komplex, haben aber erhebliche Auswirkungen: Würmer, Trojaner, Blocker, Kennwortdiebstahl, Remote-Zugriff, Vandalismus.

Ausfallzeit im Fertigungsprozess aufgrund von Malware-Vorfällen
securityincidents.net

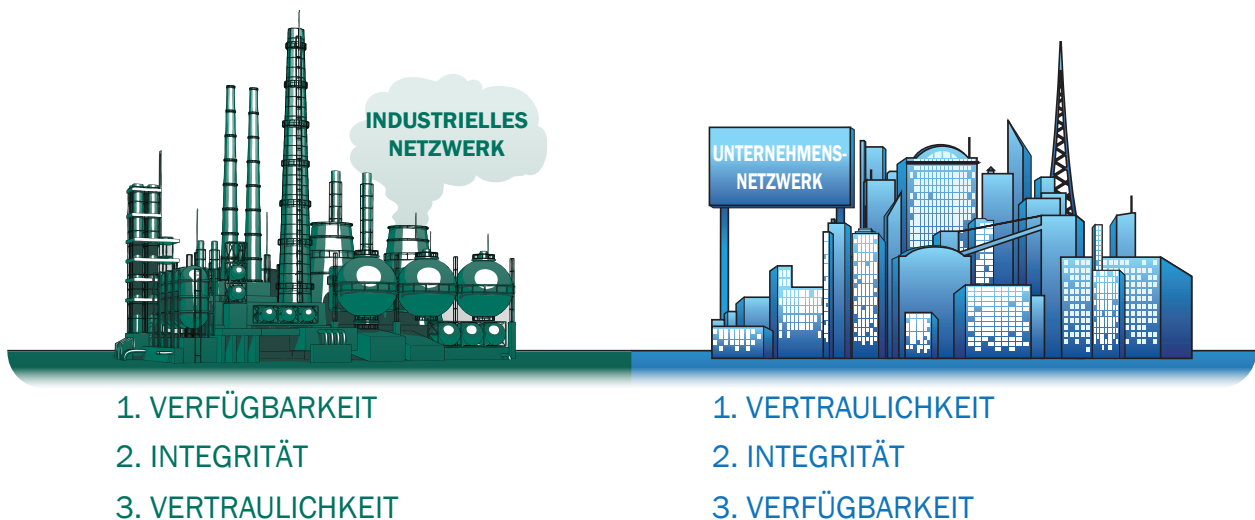
¹ SANS Institute: 2014 Control System Security Survey (Umfrage zur Sicherheit von Steuerungsanlagen)

Angriffe gegen industrielle Systeme nutzen für Start und Ausbreitung sowohl das Unternehmensnetzwerk als auch das industrielle Steuerungssystem. Energetic Bear infizierte beispielsweise die OPC-Server und Anlagensteuerungssoftware mit einem Remote-Trojaner, nutzte darüber hinaus aber auch bekannte Schwachstellen in PDF-Anwendungen von Adobe aus, um Spearphishing-Attacken zu starten. Der Angriff breitete sich von System zu System aus, entwendete dabei Informationen aus SCADA-Systemen und beschädigte ungesicherte Steuerungssysteme durch die komplette Löschung von PCs oder die Überlastung von Netzwerken.

Obwohl der Conficker-Wurm nicht speziell auf industrielle Systeme zugeschnitten ist, wurde er nicht nur in wichtigen medizinischen Anlagen gefunden, sondern war möglicherweise eine Art Wegbereiter für hochkarätige Attacken wie Stuxnet. Conficker ist in der Lage, Netzwerke vollständig zu überlasten und zentrale Prozesse zum Erliegen zu bringen. Herkömmliche Vorgehensweisen der industriellen Sicherheit gehen mit dieser Art von Bedrohung nicht sehr effektiv um: „Air-Gap“-Prozesse oder das Konzept von „Sicherheit durch Verschleierung“ lassen die Tatsache außer Acht, dass industrielle Steuerungssysteme mithilfe von Smart-Grid-Systemen und webbasierten Programmen „fast schon wie herkömmliche Verbraucher-PCs aussehen“².

INDUSTRIELLE SICHERHEIT STELLT ANDERE ANFORDERUNGEN

Bei den Bedrohungen mag es einige Überschneidungen geben, aber es gibt bedeutende Unterschiede zwischen den sicherheitstechnischen Anforderungen von industriellen Betreibern und denen von Unternehmen aus anderen Bereichen. Viele IT-Sicherheitsstrategien basieren auf dem Schutz von Daten und setzen auf Vertraulichkeit, Integrität und Verfügbarkeit (in dieser Reihenfolge). Bei industriellen Systemen steht die betriebliche Kontinuität an allererster Stelle, es geht nicht um den Schutz von Daten, sondern um den Prozess und dessen **Verfügbarkeit, Integrität und Vertraulichkeit** (in dieser Reihenfolge). Hierdurch unterscheiden sich die Sicherheitsanforderungen in diesem Sektor. Selbst die hochwertigste Sicherheitslösung ist letztendlich unbrauchbar, wenn sie die Kontinuität des betrieblichen Ablaufs gefährdet. Herkömmliche Schutzmethoden wie Malware-Schutz, Patch Management/Software-Updates und die Verwaltung der Sicherheitskonfiguration dürfen die Prozesskontinuität auf keinen Fall beeinträchtigen.



² Europäische Agentur für Netz- und Informationssicherheit (ENISA): „Can we learn from SCADA security incidents?“ (Können wir aus SCADA-Sicherheitsvorfällen lernen?)

DER RICHTIGE ANSATZ FÜR INDUSTRIELLE SICHERHEIT

Aufgrund der unterschiedlichen Anforderungen, die die industrielle Sicherheit stellt, ist die Zusammenarbeit mit dem richtigen Anbieter von entscheidender Bedeutung. Industrielle IT-Sicherheitslösungen sollten auf drei zentralen Säulen beruhen: einem prozessbasierten Ansatz für die Sicherheitsimplementierung, Sensibilisierung/Schulung der Mitarbeiter und Lösungen, die speziell für industrielle Umgebungen entwickelt werden.








Kaspersky Lab hat einen ganzheitlichen IT-Sicherheitsansatz für industrielle Systeme entwickelt, der folgende Faktoren berücksichtigt:

- Die richtige Herangehensweise: Es gibt keine Wunderwaffe oder schlüsselfertige Lösungen: Die Implementierung der IT-Sicherheit in industriellen Systemen beginnt mit Audits und anderen Services. Danach werden die Mitarbeiter auf die anstehenden Änderungen vorbereitet, gefolgt von einer schrittweisen Einführung von speziellen Lösungen, bei der der betriebliche Ablauf nicht unterbrochen wird. Nur auf diese Weise kann ein reibungsloser und voll funktionsfähiger Schutz gewährleistet werden. Da in der Fertigung jede Minute an Ausfallzeit mit beträchtlichen finanziellen Verlusten verbunden ist, muss die Installation von Produkten unter der Aufsicht von IT-Experten erfolgen, die rund um die Uhr zur Verfügung stehen.
- Mitarbeiter spielen in allen Sicherheitsstrategien eine entscheidende Rolle. Alle Akteure und Teams, vom Top-Management über die IT-Verwaltung bis hin zur Produktionstechnik, sollten durch Schulung und Sensibilisierung involviert werden. Durch ein speziell von uns entwickeltes Rollenspiel, die Kaspersky Industrial Protection Simulation (KIPS), entwickeln auch technische Laien ein Verständnis dafür, wie wichtig IT-Sicherheit ist und welche sicherheitsrelevanten Anforderungen ihr Arbeitsplatz an sie stellt.
- Auf technologischer Ebene kann Kaspersky Lab mit Lösungen aufwarten, die speziell für den Einsatz in industriellen Netzwerken entwickelt wurden – extrem fehlertolerant, störungsfrei gegenüber technologischen Prozessen und für Air-Gap-Umgebungen geeignet.

► DIE LÖSUNG VON KASPERSKY LAB

UNSER LÖSUNGSANGEBOT

EBENE 4 Geschäftsplanung und Logistik		Verwaltung der Lieferkette. Aufstellen des grundlegenden Produktionsplans: Produktion, Materialeinsatz, Lieferung und Versand.	Kaspersky Security for Business + Professional Services
EBENE 3 Verwaltung der Produktionsabläufe		Steuerung von Arbeitsablauf/ Rezeptsteuerung zur Herstellung des Endprodukts. Dokumentierung und Optimierung des Produktionsprozesses	
EBENE 2, 1 Chargensteuerung. Kontinuierliche Steuerung. Abtastregelung.		Überwachung, Leitsysteme und automatisierte Kontrolle des Produktionsprozesses	Kaspersky Industrial Security + Professional Services
		Abtastung und Regelung des Produktionsprozesses	
EBENE 0 Physisch		Physische Geräte	Physische Sicherheit

► VORTEILE FÜR DEN KUNDEN

DREIFACHER SCHUTZ

Die industriellen Sicherheitslösungen von Kaspersky Lab decken alle Aspekte der Sicherheit für Kunden aus dem industriellen Sektor ab, z. B. für Energieversorger:

- Auf jeder Ebene, vom Unternehmensnetzwerk bis hin zum Produktionsstandort.
- Schulung und Sensibilisierung für: Top-Management, IT, IT-Sicherheit und Techniker.
- Gewährleistung der betrieblichen Kontinuität durch Schutz der Daten und technologischen Prozesse.

MASSGESCHNEIDERTE SICHERHEITSOPTIONEN FÜR INDUSTRIELLE SYSTEME

Kaspersky Lab ist sich bewusst, dass jedes Technologiennetzwerk seine eigene und in den meisten Fällen einmalige Charakteristik aufweist. Unsere industriellen Lösungen basieren auf einem Baukastensystem, das vollständig anpassbar ist und auf die individuellen Anforderungen, Herausforderungen und spezifische Infrastruktur des Kunden zugeschnitten werden kann.

Durch eine Partnerschaft mit Kaspersky Lab haben unsere Kunden aus dem industriellen Sektor Zugang zu über einem Jahrzehnt an IT-Sicherheitswissen und -Expertise, denn unsere Fachleute und Techniker sind ein zentraler Bestandteil unseres Professional-Services-Teams. Da in der Fertigung jede Minute an Ausfallzeit mit beträchtlichen finanziellen Verlusten verbunden ist, muss die Installation von Produkten unter der Aufsicht von IT-Experten erfolgen, die rund um die Uhr im Einsatz sind. Zusätzlich zu Wartungsverträgen stehen Ihnen unsere Experten auch für die eingehende Untersuchung von Sicherheitsvorfällen sowie für regelmäßige Analyseberichte zu vorhandenen Bedrohungen zur Verfügung. Hierzu gehören auch die Bedrohungsanalysen von unseren Experten aus dem GRaT-Team. Wir bei Kaspersky Lab sind der Auffassung, dass eine wirkungsvolle IT-Sicherheit für den industriellen Sektor erst durch eine Kombination aus Technologie und integrierten professionellen Services entsteht. Zu den von Kaspersky Lab angebotenen professionellen Services gehören:

- IT-Sicherheitsprüfungen, Berichte und Empfehlungen, gefolgt von der Entwicklung und Umsetzung von Richtlinien und Verfahren sowie der erforderliche technische Support.
- Entwicklung von Bedrohungsmodellen und Empfehlungen zur Risikominderung
- Vorfallsreaktion: Untersuchung, digitale Forensik (mit Malware-Analyse) und rechtlicher Beistand.
- Schulung in ICS-spezifischer und allgemeiner IT-Sicherheit
- Beratung von staatlichen Stellen und Genehmigungsbehörden

KASPERSKY LAB: DIE ZUKUNFT DER INDUSTRIELLEN SICHERHEIT

Aufbauend auf unserer langjährigen Erfahrung mit industriellen Sicherheitstechnologien entwickelt Kaspersky Lab maßgeschneiderte Lösungen für den Schutz von Technologiennetzwerken. Zur langfristigen Strategie von Kaspersky Lab gehört die Entwicklung eines sicheren Betriebssystems, womit wir unsere Vision einer ultimativen, integrierten Sicherheitslösung für eine Vielzahl unterschiedlicher SPS-basierter Geräte unterstreichen, die in wichtigen Infrastrukturen, darunter auch Industrieanlagen, eingesetzt werden. Als verlässlicher IT-Sicherheitsanbieter für führende

Industrieunternehmen, die unsere Virenschutzlösungen bereits seit vielen Jahren nutzen, arbeitet Kaspersky Lab überdies mit Anbietern aus dem Bereich der industriellen Automatisierungstechnik zusammen, darunter Emerson, Rockwell Automation, Siemens etc. Unser gemeinsames Ziel ist die Entwicklung spezieller Verfahren und IT-Sicherheitsframeworks zum Schutz von industriellen Systemen vor vorhandenen und aufkommenden IT-Bedrohungen (einschließlich APTs) und die Kompatibilität von Kaspersky-Lösungen mit der Betriebstechnik unserer Kunden. Dies demonstriert unsere Fähigkeit, wirkungsvolle industrielle Sicherheitslösungen zu entwickeln, die die betriebliche Kontinuität und Konsistenz nicht beeinträchtigen.

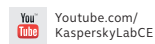
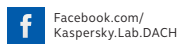
KASPERSKY LAB – FACHLEUTE FÜR INDUSTRIELLE SICHERHEIT

Laut einer Studie von Forrester Research können die Bedrohungen für wichtige industrielle Infrastruktureinrichtungen nicht länger ignoriert werden. Bei der Auswahl eines Sicherheitsanbieters sollte deshalb, „speziell auf Know-how im Bereich industrielle Sicherheit geachtet werden.“³ Die Forrester-Studie nennt Kaspersky Lab als einen der wenigen Anbieter von speziellen industriellen Sicherheitslösungen, die ihr Versprechen tatsächlich halten können und über echte Erfahrung und Expertise in diesem Sektor verfügen.

Als anerkannter Vorreiter bei IT-Sicherheit und Schutz von industriellen Systemen ist Kaspersky Lab mit der kontinuierlichen Weiterentwicklung von Lösungen beschäftigt, die mehr leisten, um mit den sich ständig weiterentwickelnden Bedrohungen von industriellen Anlagen und wichtigen Infrastrukturen umzugehen. Beginnend bei der Betriebsführung bis hin zur SCADA-Ebene und darüber hinaus, in eine Zukunft, in der ein vollständig geschütztes Betriebssystem einmal Wirklichkeit sein wird. So trägt Kaspersky Lab entscheidend dazu bei, dass Industrie, Behörden und staatliche Stellen auf der ganzen Welt rechtzeitig auf Veränderungen in der Bedrohungslandschaft vorbereitet sind und sich effektiv verteidigen können.

Die industrielle Sicherheit hat Konsequenzen, die weit über den Schutz von Unternehmen und geschäftlicher Reputation hinausgehen. In vielen Fällen spielen beim Schutz von industriellen Systemen ökologische, soziale und makroökonomische Faktoren von erheblichen Ausmaß eine Rolle. Da die Risiken für kritische industrielle Infrastrukturen zunehmen, ist die Auswahl eines geeigneten Beraters und Technologiepartners zum Schutz Ihrer Systeme so wichtig wie noch nie. Rufen Sie doch einfach einen unserer Experten bei Kaspersky Lab an und informieren Sie sich über die Zukunft der industriellen IT-Sicherheit!

³ Forrester Research, *S&R Pros Can No Longer Ignore Threats to Critical Infrastructure* (S&R-Experten dürfen Risiken für kritische Infrastrukturen nicht länger ignorieren) von Rick Holland.



Kaspersky Lab
www.kaspersky.de

Informationen zur Internetsi-
cherheit: www.viruslist.de

Informationen zu Partnern in Ihrer Nähe
finden Sie hier: www.kaspersky.de/buyoffline

© 2015 Kaspersky Labs GmbH Alle Rechte vorbehalten. Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer jeweiligen Rechtsinhaber. Mac und Mac OS sind eingetragene Marken von Apple Inc. Cisco ist eine eingetragene Marke oder eine Marke von Cisco Systems, Inc. und/oder seinen Tochtergesellschaften in den USA und bestimmten anderen Ländern. IBM, Lotus, Notes und Domino sind Marken der International Business Machines Corporation und als solche in vielen Rechtsgebieten weltweit eingetragen. Linux ist das eingetragene Markenzeichen von Linus Torvalds in den USA und anderen Ländern. Microsoft, Windows, Windows Server und Forefront sind eingetragene Marken der Microsoft Corporation in den USA und anderen Ländern. Android™ ist eine Marke von Google, Inc. Die Marke BlackBerry ist Eigentum von Research In Motion Limited und in den USA eingetragen sowie als solche in anderen Ländern eingetragen bzw. ihre Eintragung wurde beantragt.

