„human firewall“

Die Zukunft der Unternehmenssicherheit im digitalen Zeitalter!

Florian Haacke, Leiter Konzernsicherheit der innogy, im Gespräch mit SECURITY *insight* über neue Herausforderungen

Florian Haacke, Leiter der Konzernsicherheit innogy SE

SECURITY *insight*: Herr Haacke, in der Community kennt man Sie als Sicherheitschef von RWE - jetzt leiten Sie die Konzernsicherheit der innogy SE! Was ist passiert?

Florian Haacke: Anfang 2016 ist die innogy SE im Zuge einer Umstrukturierung des RWE-Konzerns entstanden. Hinter der neuen Marke innogy steht ein etabliertes europäisches Energieunternehmen – seit dem erfolgreichen Börsengang im Herbst vergangenen Jahres übrigens das wertvollste Energieunternehmen Deutschlands – mit rund 40.000 Mitarbeitern mit hoher Expertise und gleichzeitig neuen Ideen und modernen Geschäftsmodellen. Mit seinen drei Geschäftsfeldern Erneuerbare Energien, Netz & Infrastruktur sowie Vertrieb steht innogy für eine moderne, dekarbonisierte, dezentrale und digitale Energiewelt. Insbesondere die in die Zukunft gerichtete, digitale Energiewelt in Kombination mit der kritischen Infrastruktur der Strom- und Gasnetze sowie radikalen Innovationen ist für mich aus Sicherheitsgesichtspunkten sehr vielfältig und ich freue mich, dass unser Sicherheitsteam seine Stärken hier voll einbringen kann.

Sicherheit, Kritische Infrastrukturen und radikale Innovation – wie passt das zusammen?

Die Energiewelt ist bereits seit einiger Zeit erheblichen Veränderungen ausgesetzt. Themen wie Industrie 4.0 und Internet of Things, dezentrale Energieerzeugung und Elektromobilität werden dabei nicht zuletzt den Netzbereich fordern. Darauf ist die Konzernsicherheit mit einer zukunftsfähigen Sicherheitsstruktur sehr gut vorbereitet und unterstützt die Geschäftsfelder intensiv mit einem starken Fokus auf das Thema Cybersicherheit.

Was verstehen Sie unter zukunftsfähigen Sicherheitsstrukturen?

Unseren umfangreichen Transformationsprozess in der Konzernsicherheit haben wir –. damals noch bei RWE – 2013 begonnen. Das übergeordnete Ziel war ein zukunftsorientiertes, leistungsfähiges und schlankes Security-Setup bei voller Kostentransparenz und gleichzeitiger Realisierung monetärer Einsparungen, natürlich ohne jegliche Abstriche bei der Sicherheit zu machen. Nach einer konzernweiten, länderübergreifenden Bündelung sämtlicher Sicherheitsfunktionen im Konzern, sowie der damit einhergehenden systematischen Erfassung sämtlicher zentraler und dezentraler Sicherheitskosten haben wir für alle Security-Themen zunächst „Make or Buy“-Entscheidungen getroffen und alle wesentlichen nicht kerngeschäftsrelevanten Themen auf „Buy“ gesetzt. Mit über 100 unterschiedlichen Projekten war es uns möglich, die Konzernsicherheit nachhaltig um über 30% zu reduzieren; ohne zusätzliche Risiken einzugehen! Durch Effizienzsteigerungsmaßnahmen in allen Securitybereichen waren wir dann in der Lage, die dadurch freiwerdenden Ressourcen ohne Kostensteigerung in die nachhaltige und andauernde Stärkung der Cyber Security zu verschieben. Ohne die physischen Sicherheitsthemen zu vernachlässigen – diese bilden auch weiterhin das solide Fundament unserer Tätigkeit – ist Cyber Security durch den andauernden und zunehmenden Digitalisierungstrend in allen Unternehmen das Top-Thema, mit steigender Bedeutung.

Aber liegt die Verantwortung für IT-Sicherheit nicht in der IT?

Das hängt davon ab, wie Sie Verantwortung definieren. Für ein Unternehmen, dessen Kerngeschäft nicht IT ist, bei dem IT also „Commodity“ ist, ist aus Governance-Gesichtspunkten ganz sicher eine Funktionstrennung sinnvoll und zeitgemäß. Wie das aussehen kann, haben wir 2015 in einem von uns angestoßenen aber gemeinsam mit der IT durchgeführten Projekt definiert, Vorgabe und Überwachung, also Governance, von der Verantwortung für den tatsächlichen IT-Betrieb zu trennen. Mit Vorstandsentscheidung ging dann Anfang 2016 die IT-Security Governance vom CIO auf den CSO, also die Konzernsicherheit, über. Die nun eindeutig zugeordnete Verantwortung hilft allen Beteiligten und wir ziehen alle an einem Strang – jeder in seiner Rolle.

Wie müssen wir uns die Cyber Security Experten bei innogy vorstellen?

Die mehr als 30 Experten, die wir im Bereich Cyber Security der Konzernsicherheit gebündelt haben, bedienen grundsätzlich ganz unterschiedliche Themenschwerpunkte. Neben der klassischen Informationssicherheit haben wir Experten für IT- und OT-Security sowie Experten, die einen gutachterlichen Expertenstatus haben und unser Cyber Security Incident Response Team (CSIRT) bilden. Der Bereich Cyber Security gehört zu den trainingsintensivsten Themenfeldern, um in diesem komplexen und sich stetig verändernden internationalen Umfeld bestehen zu können. Hier investieren wir enorm in die kontinuierliche Qualifizierung unserer Mitarbeiter. Zudem haben wir unmittelbar mit der Entscheidung der Bundesregierung, das IT-Sicherheitsgesetz Mitte 2015 in Kraft zu setzen, ein Team aus weiteren 10 Experten mit Zertifizierungserfahrung aufgebaut, um unsere kritischen Infrastrukturbereiche im Konzern bei der Vorbereitung, Durchführung, Nachbereitung und anschließender Aufrechterhaltung der gesetzlich bis Ende Januar 2018 geforderten externen IT-Sicherheits-Zertifizierung zu unterstützen. Auch für Unternehmen wir das unsere, das seit Jahren im Thema Sicherheit gut aufgestellt ist und sich sehr früh an international anerkannten Standards orientiert hat, bedeutet die externe Zertifizierung in einem so kurzen Zeitrahmen doch einen erheblichen Kraftakt.

Welche Bedeutung haben gesetzliche Security Auflagen heute und in der Zukunft?

Persönlich bin ich der Auffassung, dass die unternehmerische Verantwortung das Thema Sicherheit vollumfänglich einschließt und bin daher kein „Fan“ von zunehmender Regulierung. Für international tätige Unternehmen sind nationalstaatliche Alleingänge selten vorteilhaft. Es gilt daher, an der Entwicklung internationaler Standards mitzuwirken, die Sicherheit erzeugen und gleichzeitig Wettbewerb ermöglichen. In der Realität nimmt die Sicherheitsregulierung aber dramatisch zu und wird weiter steigen. Und dieser Realität müssen wir uns immer wieder stellen. Was mit dem IT-Sicherheitsgesetz in Deutschland gestartet ist, setzt sich über die europäische NIS-Richtlinie fort. Und nicht jede Auflage ist verkehrt. Manchem Sicherheitsbereich mag sie sogar eine gesetzliche Grundlage für ggf. fehlende Budgets und Ressourcen bieten. Aber natürlich ist immer auch Bürokratie damit verbunden, deren Erfüllung keinen Mehrwert für die Sicherheit bietet. Im Gegenteil. Auch diese kostet wertvolle Ressourcen, die ich gerne für tatsächlich sicherheitsrelevante Fragestellungen übrig hätte. In Europa bekommen wir aktuell noch mehr gesetzlichen „Rückenwind“, zum einen mit der EU Trade Secret Directive aber natürlich auch durch die viel prominentere EU-Datenschutzgrundverordnung. Verbunden mit den gesetzlichen Sanktionsmöglichkeiten erhalten diese Themen eine hohe Aufmerksamkeit des Topmanagements. Vor diesem Hintergrund freue ich mich natürlich besonders, das jüngst auch der Konzerndatenschutz an die Konzernsicherheit angebunden wurde. Das macht einfach Sinn.

Was bleibt denn Ihrer Meinung nach von klassischen Sicherheitsthemen wie Objektschutz, Veranstaltungsschutz oder Reisesicherheit übrig? Und welche Rolle spielen die Mitarbeiter?

Diese Themen haben weiterhin ihre Berechtigung und werden daher auch fester Bestandteil des Portfolios jedes Sicherheitsverantwortlichen bleiben. Aber ihr Stellenwert ändert sich. Der Trend geht eindeutig in Richtung Prozess-Sicherheit und –stabilität und diese werden immer digitaler. Wenn ich mit dieser Einschätzung richtigliege, dann dürfte neben Cyber Security und Datenschutz zukünftig auch das Thema Business Continuity in der Bedeutung weiter steigen. Bei all der Bedeutung, die der Megatrend Digitalisierung heute und in Zukunft hat: Diese wird durch Menschen und Mitarbeiter gestaltet, die sensibilisiert und geschult werden müssen, um ein ausgewogenes Verständnis für Licht und Schatten sowie Chance und Risiko zu bewahren. Mit unserer „human firewall“ Kampagne sind wir in sieben Sprachen konzernweit unterwegs, um Aufsichtsräte, Vorstände, Führungskräfte und Mitarbeiter mit bewährten Formaten aber auch neueren Dialogformaten wie z.B. Diskussionsrunden zur Mittagszeit („unsere Lunch´n Learns“), zu erreichen. Im Mittelpunkt der Kampagne steht der Mitarbeiter selbst, der sich mit persönlichem Foto und einem „Sicherheitsversprechen“, dem sogenannten Cyber Pledge, in unsere immer länger werdende human firewall bei innogy einreihen kann. Das unterstreicht: Jeder ist aktiver Teil der Sicherheitsstrukturen in unserem Unternehmen.