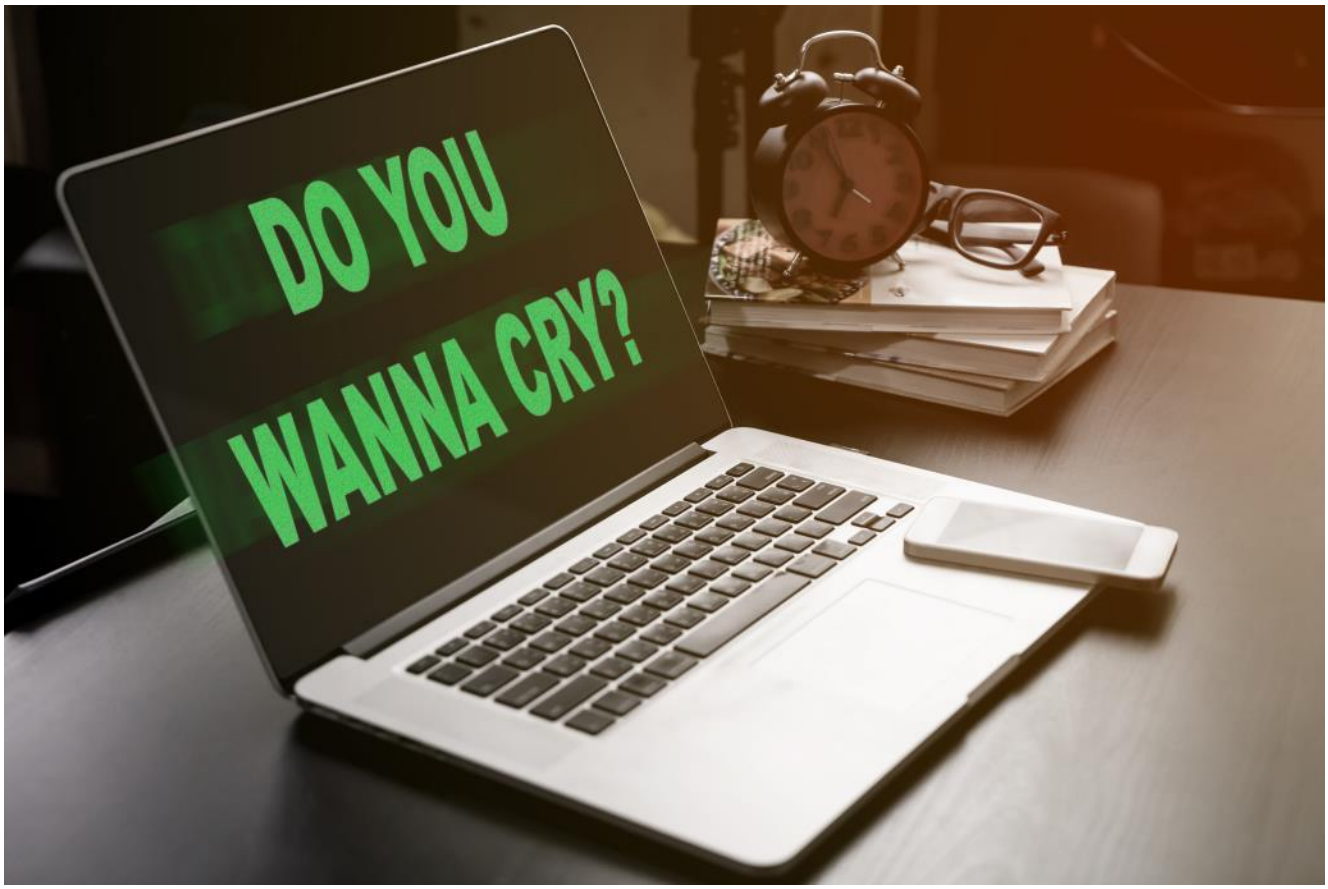
esatus AG
Enforcing Information Security

IT Security – Cyberangriffe 2016/2017

Cyberangriffe sind in der heutigen Zeit nicht mehr nur fiktive Szenarien, sondern gehören längst zu realen Bedrohungen für Unternehmen und Privatpersonen. Dagegen gilt es sich zu schützen. Das Thema Information Security nimmt in Zeiten von Digitalisierung aller Lebens- und Geschäftsbereiche sowie der Industrie 4.0 einen immer höheren Stellenwert ein.
Dieses Whitepaper befasst sich mit den aktuellen Trends in Sachen Cyberangriffe und erläutert, wie man sich gegen diese erfolgreich schützen kann.



Die Ransomware „WannaCry“ war wohl einer der bekanntesten Vorfälle 2017 in Sachen Cyberangriffe.

Der Begriff der IT-Sicherheit

IT-Sicherheit beschäftigt sich mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.
Sie hat die Aufgabe, Unternehmen und deren Werte gegenüber Bedrohungen zu schützen und wirtschaftliche Schäden durch Verletzung von Vertraulichkeit, Integrität und Verfügbarkeit der Systeme zu verhindern.

Schutzziele der IT-Sicherheit

In der IT-Sicherheit gilt es, verschiedene Schutzziele zu wahren. Die wichtigsten dieser Schutzziele werden im Folgenden vorgestellt.

Vertraulichkeit (engl. confidentiality):
Informationen dürfen nur autorisierten Personen zugänglich sein. Der Schutz vor unautorisierter Informationsgewinnung ist notwendig. Maßnahmen, um die-

ses Schutzziel zu bewahren, sind z. B. Verschlüsselung von Daten, Zugriffskontrollen oder Informationsflusskontrollen.

Integrität (engl. integrity):
Daten müssen korrekt, vollständig und unverfälscht sein. Der Schutz vor unautorisierter und unbemerkter Modifikation von Daten ist hier notwendig. Maßnahmen, um dieses Schutzziel zu bewahren, sind z. B. Unterscheidung und Zuordnung von Lese- und Schreibberechtigungen auf Daten, Manipulationserkennung durch z. B. Prüfwerte mittels kryptografischer Hashfunktionen oder gesicherte Aufbewahrung von Kopien zum späteren Abgleich mit den Originalen.

Verfügbarkeit (engl. availability):
Die Funktionen eines IT-Systems müssen ständig bzw. innerhalb einer vorgegebenen Zeit zur Verfügung stehen. Es muss sichergestellt werden, dass die Funktionalitäten nicht vorübergehend oder dauerhaft beeinträchtigt werden.
Maßnahmen, um dieses Schutzziel zu bewahren, sind z. B. Datensicherung (Backups und Redundanzen), Vertretungsregeln, Regelung und Schutz vor Überlastung.

Authentizität (engl. authenticity):
Authentizität ist zu verstehen als die Nachweisbarkeit der Identität eines Objektes oder einer Person. Der Urheber von Daten oder Nachrichten ist vom Empfänger eindeutig identifizierbar und nachprüfbar. Maßnahmen, um dieses Schutzziel zu bewahren, sind z. B. Ausstellung und Überprüfung von Zertifikaten oder Token, biometrische Verfahren, elektronische Signaturen oder händisches Unterschreiben eines Dokumentes.

Nichtabstreitbarkeit (engl. non repudiation):
Der Ersteller von Daten kann die Erzeugung im Nachhinein nicht abstreiten. Der Schutz vor unzulässigem Abstreiten durchgeführter Handlungen ist hier notwendig. Maßnahmen, um dieses Schutzziel zu bewahren, sind z. B. elektronische Signaturen, händische Unterschrift oder Protokollierung von Aktionen mit den dazugehörigen Zeitpunkten in Log-Dateien.

Privatheit (engl. privacy):
Privatheit ist die Gewährleistung des informationellen Selbstbestimmungsrechts und der Privatsphäre. Maßnahmen, um dieses Schutzziel zu bewahren, sind z. B. Regeln zur Datensparsamkeit, Festlegung der Zweckbindung der erhobenen Daten, Anonymisierungsverfahren oder Pseudonyme.

Was ist Ransomware?

Ransomware (engl. *Ransom* für Lösegeld), oft auch als Erpressungstrojaner bezeichnet, verschlüsselt Daten auf dem Gerät des Opfers oder blockiert gänzlich den Zugriff auf das Gerät. Für die Freigabe der Daten fordern die Erpresser eine gewisse Summe an Lösegeld, welche in Form von elektronischen Zahlungsmitteln, wie z. B. Paysafe-Cards oder Bitcoin, bezahlt werden soll. Es ist ein Angriff auf die Schutzziele Verfügbarkeit und Integrität.
Ransomware wird als Anhang per E-Mail, aber auch durch die Ausnutzung von Sicherheitslücken in Webbrowsern oder über Datendienste wie Dropbox verbreitet. So werden etwa E-Mails versandt, welche bspw. eine im Anhang befindliche verseuchte ZIP-Datei als Rechnung oder Lieferschein tarnen. Andere Formate, wie Excel, Word, und PDF Dateien, können auch Ransomware enthalten.
Obwohl der Anteil von Ransomware weniger als ein Prozent aller Schadsoftware beträgt, wird 2016 nicht umsonst als das Jahr der Ransomware bezeichnet. Der Erpressungstrojaner findet seine Popularität nicht in der Verbreitungszahl, sondern in dem immensen Schaden, den er verursacht. Kommt es zum Produktionsausfall, gehen die Verluste schnell in die Höhe. Selbst wenn die Firmen die geforderte Summe zahlen, gibt es keine Garantie, dass die betroffenen Dateien wiederherstellbar sind.

Was ist eine DDoS-Attacke?

Eine DDoS-Attacke (Distributed Denial of Service) ist ein Angriff auf das Schutzziel Verfügbarkeit. Bei einem DDoS werden meist mehrere tausend gekaperte Computer missbraucht, um z. B. auf eine bestimmte

Webseite zuzugreifen. Bedingt durch die große Masse an Anfragen steigt die Systemauslastung so stark an, dass keine neuen Anfragen mehr beantwortet werden können oder das System seinen Dienst vollständig einstellt. Selbst wenn das System, dank automatisierter Skalierung, die Anzahl an Anfragen bewältigen könnte, ist auch die Bandbreite irgendwann erschöpft, sodass neue Anfragen nicht mehr bis zum System gelangen.

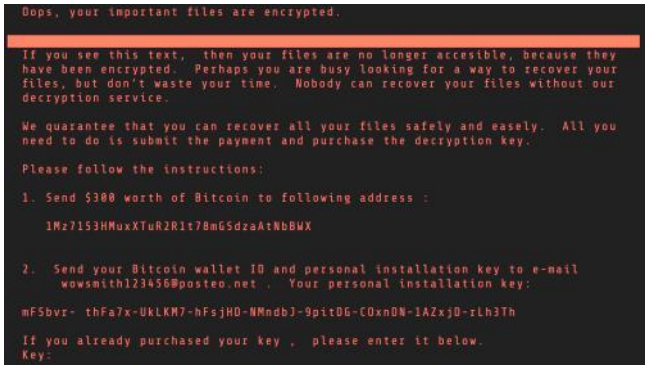
Die Ransomware WannaCry

Was ist passiert? WannaCry ist ein Schadprogramm für Windows, das im Mai 2017 für einen schwerwiegenden Cyberangriff genutzt wurde und über 230.000 Computer in 150 Ländern infizierte.
Der Angriff wurde von Europol hinsichtlich seines Ausmaßes als noch nie da gewesenes Ereignis beschrieben.

Die Liste der betroffenen global tätigen Unternehmen ist lang:

- Der spanische Telekommunikationskonzern Telefónica
- Teile des britischen National Health Service (NHS) mit mehreren Krankenhäusern
- Der US-Logistikunternehmen FedEx
- Der französische Automobilkonzern Renault
- Der japanische Automobilhersteller Nissan in Großbritannien
- Die Deutsche Bahn mit Logistiktochter Schenker
- Der chinesische Ölkonzern PetroChina
- Das Außenministerium in Rumänien
- Mehr als 1000 Computer des Innenministeriums (MWD) in Russland, das Katastrophenschutzministerium sowie das Telekommunikationsunternehmen MegaFon

Wie ist es passiert? Nach Befall eines Computers verschlüsselte WannaCry bestimmte Benutzerdateien des Rechners und forderte den Nutzer dazu auf, einen bestimmten Betrag in Bitcoin zu zahlen. Außerdem versuchte das Programm, als Computerwurm weitere Windows-Rechner zu infizieren.
Ist ein Gerät erstmal befallen, sucht WannaCry im lokalen Netzwerk nach weiteren ungeschützten Rechnern, infiziert diese und sendet Anfragen ins Internet, um auch darüber ungeschützte Rechner zu infizieren.
WannaCry basiert auf dem EternalBlue Exploit – einer Möglichkeit zur Schwachstellenausnutzung – im SMB-Protokoll (Server Message Block) von Microsoft. Dieses ist ein Netzwerkprotokoll für Datei-, Druck- und andere Serverdienste und bekannt für die Dateifreigabe. Der US-amerikanische Auslandsgeheimdienst NSA nutzte diese Lücke über mehr als fünf Jahre für eigene Zwecke, ohne Microsoft über diese zu informieren. Erst nachdem die NSA erfahren hatte, dass das Wissen über EternalBlue gestohlen wurde, informierte sie Microsoft über die Sicherheitslücke. Microsoft stellte daraufhin einen Sicherheits-Patch zur Verfügung, der jedoch bei weitem nicht bei allen Privatleuten sowie Unternehmen ausgeführt wurde, da diese die automatische Aktualisierungsfunktion nicht benutzten.



Die Ransomware Petya

Was ist passiert? Petya ist ein Erpressungstrojaner, welcher im Gegensatz zu anderen Verschlüsselungstrojanern das Inhaltsverzeichnis der Festplatten (die sogenannte Master File Table) sowie das erste Kilobyte der Dateien verschlüsselt.
Forscher und IT-Spezialisten fanden mehrere Schwachstellen im Verschlüsselungsprozess, sodass Dateien und Systeme ohne Zahlung des Lösegeldes wiederhergestellt werden konnten.
In den Jahren 2016 und 2017 tauchten so immer mehr Varianten des Trojaners auf, welche versuchten, die Verschlüsselung zu optimieren.

Der Angriff im Jahr 2017 galt hauptsächlich Unternehmen mit Sitz in Russland und der Ukraine:

- Rosneft, Bashneft und Nivea in Russland
- In der Ukraine war die Zentralbank betroffen, es kam zu Beeinträchtigungen an Kiews Flughafen und das Regierungsnetzwerk war offline.
- Durch die ukrainische Buchhaltungssoftware „M.E.Doc" sind auch deutsche Unternehmen wie Beiersdorf betroffen, die dänische Reederei Maersk, der russische Ölproduzent Rosneft, der amerikanische Pharmakonzern Merck Sharp & Dohme sowie der Lebensmittelproduzent Mondelez (Milka, Oreo).
- Der britische Konzern Reckitt-Benckiser (Sagrotan, Scholl, Nurofen, Vanish, Finish) schätzt den verursachten Umsatzverlust auf 100 Millionen Pfund. Die Malware legte unter anderem Herstellungs- und Ordersysteme lahm und schränkte auch den Warenversand des Herstellers ein.

Wie ist es passiert? Petya wurde per E-Mail übertragen und als Bewerbungsschreiben getarnt. In der E-Mail befand sich ein Dropbox-Link, der vortäuschte, dass es sich um eine Bewerbung handelt. In Wirklichkeit jedoch führte der Link zu einem als PDF-Datei getarnten Programm. Wurde diese Datei heruntergeladen und ausgeführt, entpackte sich das Programm und überschrieb den ersten Teil der Festplatte, den sogenannten Master Boot Record, welches das Starten des Betriebssystems unmöglich machte.
Petya zwingt den Rechner zum Neustart und fingiert eine Überprüfung der Datei-System-Struktur. Tatsächlich wird die Hauptdatei des Inhaltsverzeichnisses der Festplatte verschlüsselt und das System kann nicht mehr lokalisieren, wo sich die Dateien auf der Festplatte befinden oder ob sie überhaupt noch existieren. Nach Beendigung des Scans wird ein Sperrbildschirm geöffnet, der Anweisungen zur Systemwiederherstellung enthält. In den Anweisungen wird das Opfer aufgefordert, mithilfe eines Tor-Browsers eine Internetseite im Darknet zu öffnen und an die dort angegebene Adresse Lösegeld in Form von Bitcoin zu zahlen.

Schutzmaßnahmen gegen Ransomware

Präventive Maßnahmen, welche der Infektion durch Ransomware vorbeugen, werden nachfolgend vorgestellt.

- Implementieren einer soliden Sicherheitslösung.
- Regelmäßige Sicherungen durchführen und auf einem vom System getrennten externen Speichermedium aufbewahren.
- Software und Betriebssystem aktuell halten um Schwachstellen zu vermeiden.
- Vorsicht bei E-Mail-Anhängen, besonders bei jenen von unbekannten Empfängern und Dateien im ZIP-Format oder Word- und Excel-Dateien.
- Eingrenzung der Verwendung von Browser-PlugIns sowie Verwendung eines Browserschutzes.

Angriff auf Dyn

Was ist passiert? Ein großer DDoS-Angriff auf die US Amerikanische Firma Dyn fand am 21. Oktober 2016 statt. Für einen großen Anbieter von DNS-Dienstleistungen (Domain Name System) ist ein Ausfall der Server natürlich fatal. Einige große Firmen, wie z. B. Amazon, Netflix, Airbnb, Twitter etc., arbeiten mit der DNS-Lösung der Firma Dyn. Die Angreifer nutzten hierbei aber kein gewöhnliches DDoS-Botnetz, sondern unter anderem Teile des auf „Mirai" basierten Botnetzes, welches ein Zusammenschluss aus mehreren hunderttausend gekaperten IoT-Geräten (also Geräte wie bspw. smarte Glühbirnen, smarte Kühlschränke, Überwachungskameras mit einer Internetschnittstelle usw.) darstellt.
Warum ist das passiert? Nicht jeder Dienstleister oder Betreiber von Webservern und Diensten rüstet sich gegen DDoS-Angriffe. Es muss immer ein gewisser Kosten-Nutzen-Faktor vorhanden sein. Im Falle der Firma Dyn gab es zwar aktive Gegenmaßnahmen, diese waren aber nicht für einen derartigen Angriff gewappnet. Kunden der Firma Dyn bekamen einige Tage zuvor Drohungen per E-Mail, die ankündigten, dass, wenn nicht eine bestimmte Summe an Bitcoin gezahlt werde, ein großer nicht abwehrbarer DDoS-Angriff stattfinden würde.

Wie hätte man das verhindern können? Es gibt verschiedene Ansätze, um solchen DDoS-Angriffen entgegenzuwirken. In vielen Fällen weisen IoT-Geräte große Sicherheitslücken auf und sind somit für Angreifer ein leichtes Ziel. Die Hersteller müssten dafür verantwortlich gemacht werden und Sorge dafür tragen, dass ihre Geräte sicher sind.
Auch sollten Webseiten auf mehrere DNS-Anbieter verteilt werden. Da Dyn selbst ein DNS-Anbieter ist, hätten die Kunden von Dyn nicht auf einen DNS-Anbieter setzen sollen, sondern auf mehrere verschiedene. Damit wäre zumindest die Verfügbarkeit der einzelnen Kunden von Dyn gewährleistet gewesen.
Eine weitere Möglichkeit ist die Gültigkeitsdauer (Time To Live) zu erhöhen. Dabei bleibt die IP-Adresse der Domain lokal länger erhalten. Dies ist aber laut dem Experten Frank Michlick nur dann eine Lösung, wenn es sich bei dem Opfer um einen DNS-Anbieter handelt.
Eine letzte Möglichkeit, um sich als Anbieter eines Webdienstes oder einer Webseite vor DDoS-Angriffen zu schützen, sind sogenannte „DDoS-Shields". Diese analysieren den Traffic auf einer Webseite und bemerken, wann ein Angriff stattfindet oder wann es legitimer Daten-Traffic ist. Wird ein Angriff festgestellt, leitet dieses „Shield" die bösartigen Anfragen auf extra dafür vorgesehenen Server um und verteilt diese auf alle Ressourcen. Somit wird ein DDoS-Angriff abgeschwächt und nutzlos.

Angriff auf Telekom Router

Was ist passiert? Etwa 900.000 Kunden der Telekom waren am 9. Dezember 2016 plötzlich vom Netz getrennt und dann für etwa zwei Tage offline. Grund dafür war der Versuch, Router, die unter anderem von der Telekom vermarktet werden, in das Mirai-Botnetz zu integrieren. Angreifer infiltrierten Router von „Zyxel" durch eine Sicherheitslücke des irischen Providers „Eir". Damit attackierten sie das Netz und versuchten ebenfalls durch die Lücke, Router (einige Geräte aus der „Speedport"-Reihe) von zumeist Telekom-Kunden zu kapern. Bei dieser Lücke handelt es sich um den TCP-Port 7547, welcher Teil des Fernwartungsprotokolls TR-069 ist.
Dieses Protokoll ist nicht dafür vorgesehen, von jedem angesprochen zu werden, da man hierüber DNS- und NTP-Einstellungen der DSL-Router mit einer simplen Anfrage ändern kann, ohne sich anmelden zu müssen. Das Protokoll sollte normalerweise nur aus dem Heimnetz des Kunden erreichbar sein. Zyxel, der Hersteller des Eir-Routers, stellte diese Funktion jedoch auf der externen Schnittstelle des Routers, also auf jene Schnittstelle, die von außen erreichbar ist, über den TR-069-Fernwartungs-Port bereit. Diese Schwachstelle in den Eir-Routern lies es zu, dass Angreifer befugt waren, mit einem Befehl zum Einfügen eines neuen Zeit-Servers, Schadcode in den Router einzuschleusen, welcher dann vom Router ausgeführt wurde.
Telekom Router waren allerdings nicht von dieser Sicherheitslücke betroffen, weshalb sie nicht Teil des Mirai-Botnetzes wurden. Die sich immer wiederholenden Angriffe brachten die Router zum vollständigen Stillstand.
Warum ist das passiert? Trotz mehrerer Hinweise von Kunden im Jahre 2014, dass der Fernwartungs-Port von außen erreichbar ist, sah die Telekom hier keine potentielle Sicherheitslücke. Deshalb haben sie diesen Port auch nicht geschlossen bzw. angepasst.
Wie hätte man das verhindern können? Die Telekom, als großes und technikaffines Unternehmen, müsste über die Gefahren einer solchen Schwachstelle wissen und diese umgehend beheben. Es muss klar sein, dass ein nach außen offener Port eine Sicherheitslücke darstellt. Die Telekom hätte den Fernwartungs-Port auf ihre Server-Adressen beschränken müssen, so dass jede andere Anfrage abgelehnt wird.

Prognosen für weitere Angriffe

Im Folgenden werden potentielle und mögliche Angriffsarten der kommenden Monate aufgelistet, welche derzeit in Fachkreisen diskutiert werden.

APT („Advanced Persistent Threat")
Das sind maßgeschneiderte Angriffe, die zielgerichtet, komplex und effektiv auf kritische IT-Infrastrukturen, z. B. von Behörden, ausgelegt sind.

Missbrauch von unsicheren IoT-Geräten

Auch weiterhin wird dies ein großes Problem sein. Viele Hersteller von IoT-Geräten vernachlässigen aus Unwissenheit oder aus Gründen der Kostenersparnis die Sicherheit ihrer Geräte. Update-Funktionalitäten werden nicht eingebaut, weil Ressourcen für Update-Server gespart werden oder die Implementierung kompliziert ist. Dadurch werden DDoS-Attacken mit mehreren GBit/s oder gar mit mehreren TBit/s an Traffic möglich, weil es immer mehr Geräte gibt, die leicht zu kapern sind.

CEO Fraud

Cyberkriminalität muss nicht immer nur auf Computersystemen stattfinden. Auch Mitarbeiter am Telefon können eine erhebliche Schwachstelle darstellen. So können Angreifer sich durch gesammelte Daten über den CEO eines Unternehmens als dieser ausgeben und z. B. eine Überweisung von einer höheren Summe Geld veranlassen. Dies findet zumeist per E-Mail oder am Telefon statt, wobei der Weg per Mail für die Angreifer einfacher ist. Eine E-Mail-Adresse lässt sich leichter fälschen als die Stimme des Chefs.

Computerkriminalität-as-a-service

Immer öfter wird im Darknet der Service angeboten, Schadsoftware zu erstellen oder DDoS-Attacken durchzuführen. Der eigentliche Angreifer muss nicht mehr eigenständig den Code programmieren, sondern nur noch für den speziell angefertigten Angriff bezahlen.

Die **esatus** AG ist ein mittelständisches IT-Beratungsunternehmen. Getreu der Unternehmensmission „Enforcing Information Security" ist die esatus AG der qualifizierte, erfahrene und flexible Ansprechpartner für Projekte rund um das Thema Informationssicherheit. Für Kunden werden optimale und individuell gestaltete Lösungen für Herausforderungen in den Bereichen Identity & Access Governance, IT Security, sowie Governance, Risk und Compliance angeboten. Zudem bietet die **esatus** AG eine umfassende Beratung zur Thematik des IT-Sicherheitsgesetzes an, beispielsweise zur Einrichtung einer Meldestruktur. Die Zufriedenheit von Kunden ist der Leitfaden, nachdem sich das gesamte Handeln des Unternehmens richtet.

Herausgeber **esatus** AG

Grafik Seite 1 © junce11/Fotolia
https://de.fotolia.com/id/152699514

Grafik Seite 3 © Creative One/Fotolia
https://de.fotolia.com/id/162683776

Weitere Informationen zum Thema „IT Security – Cyberangriffe 2016/2017" bei der **esatus** AG finden Sie unter: esatus.com

Stand der Informationen im vorliegenden Whitepaper: September 2017