LEITFADEN FÜR GANZHEITLICHE CYBER-SICHERHEIT

BEST PRACTICES & TIPPS ZUM SCHUTZ IHRES UNTERNEHMENS

F-Secure

WIE STEHT ES UM IHRE CYBER-SICHERHEIT?

Auf dem Papier ist Cyber-Sicherheit ziemlich einfach: die Integrität Ihres Systems wahren und gleichzeitig Angreifer abwehren. In der praktischen Umsetzung wird es jedoch deutlich komplizierter. Begrenzte Budgets, fehlendes Know-how und geringes Bewusstsein für verschiedene Sicherheitsthemen können Hürden für einen wirksamen Schutz gegen moderne Cyberangriffe sein.

Zu den drängendsten Problemen zählen Transparenz und Klarheit. Wie steht es aktuell um unsere Sicherheit? Was fehlt uns? Obwohl die meisten IT- und Sicherheitsexperten die Technologien und Best Practices in ihrem Bereich kennen, ist es leicht, angesichts des sich ständig verändernden digitalen Umfelds und der rapiden Entwicklung externer Bedrohungen den Blick auf das Wesentliche zu verlieren.

PRÜFEN SIE IHRE AKTUELLE SITUATION – UND VERBESSERN SIE SIE NOCH HEUTE!

Hier kommen wir ins Spiel. Wenn Sie Tipps benötigen oder Ihr Gedächtnis auffrischen möchten, was für Ihre Cyber-Sicherheit zu beachten ist, dann ist dieser Leitfaden genau das Richtige für Sie. Wir zeigen Ihnen die grundlegenden Bausteine eines stabilen Cyber-Sicherheitsprotokolls – von Risikobeurteilung über Endgeräteschutz bis hin zu Bedrohungserkennung. Prüfen Sie Ihre aktuelle Situation – und verbessern Sie sie noch heute!

1 RISIKEN BEURTEILEN

Die Risikobeurteilung ist eine Kernkomponente – und der Ausgangspunkt – jeder erfolgreichen Sicherheitsstrategie. Ein gezielt eingesetztes Protokoll wird Ihnen immer mehr bringen als ein 08/15-Ansatz. Es gibt mehrere Methoden der Risikobeurteilung, doch die folgenden Elemente sind die Grundlage für jeden tragfähigen Ansatz.

1.1 ALLE PERSPEKTIVEN BELEUCHTEN

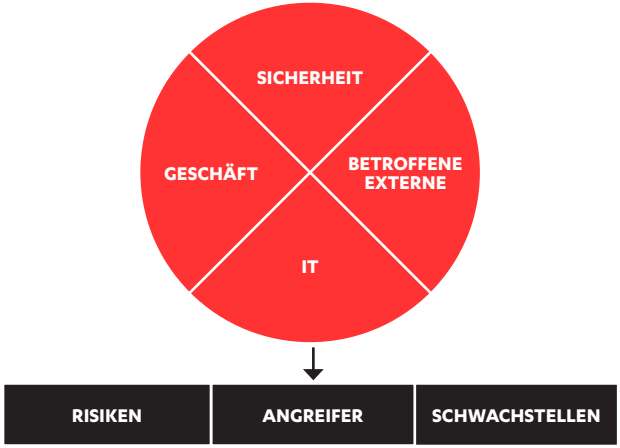
Eine gute Risikobeurteilung ist eine Aufgabe für ein funktionsübergreifendes Team. Jeder muss involviert sein – von der IT über die Sicherheitsabteilung bis hin zum Vertrieb und Marketing. Denken Sie auch daran, betroffene Externe wie Lieferanten und Anbieter einzubeziehen, da die Lieferkette einer der beliebtesten Angriffsvektoren ist, um die Verteidigungssysteme eines Unternehmens zu durchbrechen.

Nutzen Sie das breitgefächerte Fachwissen Ihres Teams, um mögliche Risiken, Schwachstellen und Angreifer zu identifizieren, und erstellen Sie in einer Brainstorming-Sitzung eine Liste.

Es klingt so naheliegend, doch nur sehr wenige Unternehmen nutzen das volle Potenzial ihres internen Know-hows, um mögliche Risiken vorherzusagen und zu identifizieren. Auch wenn der Blick nach außen sehr wichtig ist (dazu kommen wir später), erhalten Sie die wertvollsten Einblicke immer von den Menschen, die Ihre IT-Infrastruktur, Ihr Geschäftsmodell und Ihre spezifischen Probleme in- und auswendig kennen.

TIPP!

Nutzen Sie Schwachstellenmanagement-Software, um nicht nur Ihre eigene IT-Umgebung zu scannen, sondern auch die Ihrer Partner und Lieferanten. So können Sie Ihre aktuelle Sicherheitslage umfassend überprüfen.



73 %
der Datenschutzverletzung werden von externen Angreifern verursacht

50 %
aller Datenangriffe wurden von organisierten kriminellen Gruppen durchgeführt

Data Breach Investigations Report 2017 (Verizon)

67 %

der globalen Unternehmen wurden bereits angegriffen

Global Threat Report 2018
(451 Group for Thales)

3,62 Mio. $

kosteten Datenschutzverletzungen 2017 durchschnittlich

Cost of a Data Breach Study 2017 (Ponemon Institute)

1.2 BENCHMARKS

Versuchen Sie, Beispielfälle von relevanten Unternehmen zu finden, und übertragen Sie die bekannten Konsequenzen dieser Fälle auf Ihre Situation. Suchen Sie auch nach zuverlässigen Branchenstatistiken und -vergleichen.

Wie sind andere Unternehmen mit Angriffen umgegangen und wie haben sie ihre Cyber-Sicherheit organisiert? Wie lange dauert es im Durchschnitt, auf verschiedene Cybervorfälle zu reagieren? Lesen Sie Berichte, besuchen Sie Konferenzen und sprechen Sie mit Ihren Kollegen.

Tests können ebenfalls ein sinnvoller Ausgangspunkt für die Überprüfung Ihrer Sicherheitslage sein. Unseren kurzen Endgerätesicherheitstest finden Sie hier. Wenn Sie die Wirksamkeit Ihres aktuellen Protokolls umfassender prüfen möchten, können Sie unseren Cyber Security Stress Test absolvieren. Beide Tests ermöglichen einen Vergleich Ihrer Ergebnisse mit denen anderer Unternehmen Ihrer Größe in derselben Branche!

TIPP!

Achten Sie ganz besonders auf Fallstudien und Datenpunkte innerhalb Ihrer eigenen Branche – sei es Technologie, Produktion, Gesundheitswesen oder eine andere.

1.3 SZENARIEN AUSARBEITEN & ÜBEN

Sie können zukünftige Bedrohungen nicht mit vollkommener Genauigkeit vorhersagen, aber mit einer Zusammenfassung all Ihrer IT-Risiken unter einer einzigen, allumfassenden Definition ist es auch nicht getan.

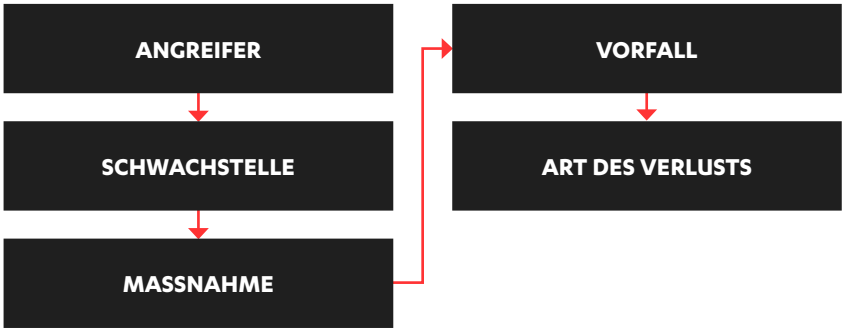
Um Risiken in Ihrem gesamten Unternehmen verständlich und behandelbar zu machen, müssen Sie umfassende Szenarien – Angreifer-Storys – erarbeiten, die die Mechanismen eines möglichen Angriffs bis ins kleinste Detail beschreiben. Welches System würde der Hacker angreifen? Wo liegen die Grenzen für Ihre finanziellen Verluste? Angreifer-Storys sollten immer auf Ihrer IT-Infrastruktur, Ihrer Branche, Ihren Datenerfassungspraktiken und Ihrem kollektiven Know-how zum Thema IT-Sicherheit basieren.

Und vergessen Sie nicht, zu üben! Wiederholte Cyber-Sicherheitsübungen sind die einzige Möglichkeit, um Ihre Reaktionsfähigkeit unter realen Bedingungen zu testen und sich für den Ernstfall zu wappnen.

77 %

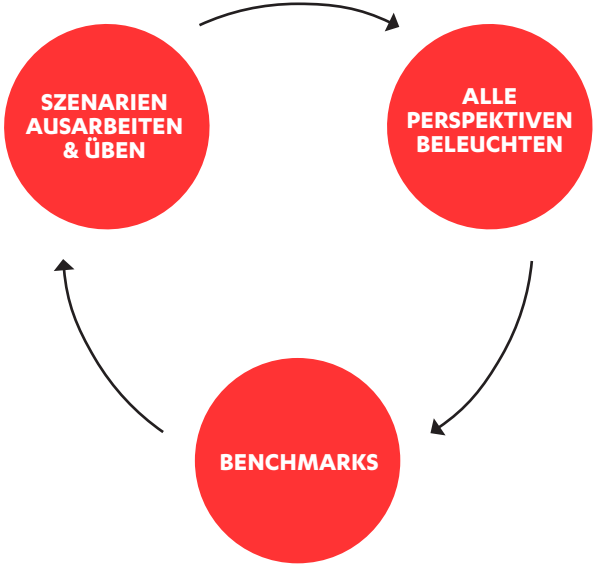
der IT-Experten sagen, dass ihre Unternehmen keine angemessenen Reaktionspläne für Vorfälle besitzen

The Third Annual Study on the Cyber Resilient Organization, März 2018. (Ponemon Institute für IBM Resilient)



TIPP!

Cyber-Sicherheitsberater können in dieser Phase ein riesiger Vorteil sein. Es ist immer gut, das Wissen und die Einblicke von Experten zu nutzen, die bereits mit zahlreichen realen Cyber-Vorfällen zu tun hatten.



1.4 ÜBERPRÜFEN & WIEDERHOLEN

Eine gute Risikoanalyse ist ein kontinuierlicher Prozess, der immer und immer wieder wiederholt wird. Irgendwas gilt es immer zu beachten: neue Bedrohungen, Angriffstrends, Technologien, Business Cases oder Prioritäten.

Nur wenn Sie einen erfolgreichen Kreislauf aus den vorgenannten drei Schritten geschaffen haben, können Sie Ihre Sicherheit im Griff behalten. Machen Sie ihn sich zur Gewohnheit! Monatliche IT-Risiko-Besprechungen können zunächst etwas bedrückend wirken, doch sie zahlen sich langfristig aus.

Ein sorgfältiger, langfristiger Ansatz wird Ihnen auch eine gute Priorisierung und Nachverfolgung Ihrer Aktivitäten ermöglichen. Sie können nicht all Ihre Schwachstellen in einem Monat korrigieren. Wenn Sie sich aber eine nach der anderen vornehmen, machen Sie langsame und stetige Fortschritte. Und darauf kommt es wirklich an!

TIPP!

Nehmen Sie regelmäßig Schwachstellen-Scans vor und verwenden Sie Software, mit der Sie einfache, leicht lesbare Berichte erstellen können, um Ihren Fortschritt von Monat zu Monat nachzuverfolgen.

2 GRUNDLAGEN UMSETZEN

Nachdem Sie Ihre IT-Infrastruktur und Problempunkte identifiziert haben, ist der nächste Schritt die Umsetzung von Sicherheitsmaßnahmen. Sorgen Sie zuallererst für den Schutz Ihrer Geräte, Software, Mitarbeiter und Netzwerke.

2.1 IHRE GERÄTE SICHERN

ENDGERÄTE SCHÜTZEN

Sichern Sie zunächst alle Endgeräte, die anfällig für Malware sind: Neben PCs, Macs, Tablets und Smartphones benötigen auch E-Mail-Server und andere Geräte Schutz. Zentralisieren Sie im Idealfall die Verwaltung Ihrer Geräte so gut es geht.

DATENVERKEHR SICHERN

Eine moderne Firewall zum Schutz des ein- und ausgehenden Verkehrs ist ebenso wichtig wie erstklassige Malware-Erkennungsraten. Hierfür ist unbedingt eine Kombination aus traditionellen Antivirenprogrammen und verhaltensbezogenen Erkennungstechnologien erforderlich.

INFEKTIONEN VORBEUGEN

Schützen Sie sich vor beliebten Angriffsvektoren, indem Sie Sicherheitsvorkehrungen gegen Infektionen mittels Browsing, E-Mails und tragbarer Geräte (USB-Geräte) treffen. Hardware-Diebstahl ist immer eine Gefahr. Richten Sie daher eine automatische Bildschirmsperre, Festplatten- und Speicherkartenverschlüsselung sowie eine Remote-Löschfunktion für Ihre Geräte ein.

TIPP!

Bei Software-Käufen oder -Upgrades achten Sie ganz besonders auf externe Bewertungen. Halten Sie nach Lösungen Ausschau, die zuverlässig Jahr für Jahr beste Ergebnisse erzielen.

>100 Millionen **neue Malware-Muster kommen jedes Jahr hinzu**

Malware Statistics (AV Test)

2.2 IHRE SOFTWARE SICHERN

ANGRIFFSFLÄCHE VERKLEINERN

Entfernen Sie Software, die Sie nicht mehr nutzen, und deaktivieren Sie unwichtige Funktionen. Verkleinern Sie Ihre Angriffsfläche weiter, indem Sie jedes System für eine spezifische Aufgabe nutzen. So lassen sich Systeme leichter sichern. Am besten lässt sich Ihre IT-Umgebung verwalten, wenn sie von vornherein so klein und effizient wie möglich gehalten ist.

BETRIEBSSYSTEM NUTZEN

Nutzen Sie die eingebauten Sicherheitsfunktionen, Datenschutz-einstellungen und Software Ihres Betriebssystems. Mehrschichtige Sicherheit bis hin zur Betriebssystemebene gibt Ihnen mehr Möglichkeiten, Angreifer abzuwehren.

PATCHES VERWALTEN

Installieren Sie Updates, sobald sie verfügbar sind – ausnahmslos. Systematisieren Sie den Prozess, sodass Ihre IT- und Sicherheitsteams jederzeit den Sicherheitsstatus aller Geräte kennen.

TIPP!

Am besten ist es, wenn Sie Ihre Software-Sicherheit weitestgehend automatisieren. Ein korrekt automatisiertes Patch-Management verhindert z. B. mehr Angriffe, als Sie sich vorstellen können.

81 %

der Schwachstellen konnten bereits am Tag ihres Bekanntwerdens durch Patches behoben werden

Vulnerability Review 2018 (Flexera)

2.3 IHRE MITARBEITER SCHÜTZEN

OPSEC AUFRECHTERHALTEN

Informieren Sie Ihre Mitarbeiter über gute Praktiken der Betriebssicherheit (OpSec; Operations Security) und heben Sie die größten Risiken für Ihr Unternehmen anhand von Beispielen hervor – von Malware bis hin zu Social Engineering. Fangen Sie an, Zugangsdaten zu überprüfen, und konzentrieren Sie sich auf Anomalien: Wenn jemand unerwartet mitten in der Nacht zur Arbeit kommt, markieren Sie dies und forschen Sie nach. Dokumentieren Sie auch gestohlene/verloren gegangene Geräte!

PASSWÖRTER SICHER MACHEN

Setzen Sie strenge Passwortrichtlinien im gesamten Unternehmen durch. Verlangen Sie verpflichtend, dass Betriebssystem- und sonstige System-Passwörter Zahlen, Sonderzeichen und Großbuchstaben enthalten, und aktivieren Sie stets die Zwei-Faktor-Authentifizierung für externe Cloud-Dienste.

KOMMUNIKATION KONTROLLIEREN

Legen Sie klare Kommunikationsprotokolle fest, insbesondere in Bezug auf Filesharing. Machen Sie eine Liste aller erlaubten Tools und Services, die zum Teilen von Informationen – intern wie externen – verwendet werden dürfen. Am besten verschlüsseln Sie zusätzlich alle sensiblen Daten.

TIPP!

Investieren Sie in eine zentral implementierte Passwort-Management-Software, die sich über alle Geräte Ihrer Mitarbeiter hinweg synchronisiert. So minimieren Sie das Risiko, dass Passwörter durchsickern oder geknackt werden.

72 %

der Unternehmen waren bereits Opfer von Phishing-Angriffen

nThreat Landscape Survey 2017: Users on the Front Line (Sans Institute)

81 %

der Datenschutzverletzungen durch Hacker nutzen gestohlene und/oder schwache Passwörter

Data Breach Investigations Report 2017 (Verizon)

2.4 IHR NETZWERK SICHERN

ZUGRIFF EINSCHRÄNKEN

Schließen Sie alle Protokolle und Ports, die nicht unbedingt benötigt werden. Schränken Sie die Benutzerrechte für kritische Systeme und Software ein und entfernen bzw. beschränken Sie Fernzugriffsfunktionen. Denken Sie auch daran, standardmäßig eingerichtete Konten des Betriebssystems zu deaktivieren oder zu ändern, da diese oft ernsthafte Sicherheitsrisiken darstellen.

VPN NUTZEN

Sichern Sie den kompletten ein- und ausgehenden Verkehr mit einem unternehmensweiten VPN (auch für mobile Geräte) und überwachen bzw. überprüfen Sie regelmäßig die Netzwerk-Protokolle auf verdächtige Aktivitäten. Sie können die Internetverbindung auch vollständig beenden, wenn sie für die Produktionsprozesse nicht benötigt wird, und so eine „Lücke" zwischen Ihren Systemen und dem Internet schaffen.

WLAN-ROUTER WARTEN

Konfigurieren Sie Ihre WLAN-Router auf die höchstmögliche Sicherheitsstufe und legen Sie besonderen Wert auf ihre Wartung, damit Angreifer Ihre Endgeräte nicht vollständig umgehen können. Spielen Sie Patches und Bugfixes unbedingt immer schnellstmöglich ein.

TIPP!

Fällt es Ihnen schwer, unter Millionen von Netzwerkereignissen Anomalien zu erkennen? Eine EDR-Lösung (Endpoint Detection & Response) ersetzt den Großteil der manuellen Arbeit und liefert Ihnen präzisere Ergebnisse dank KI, maschinellen Lernens und modernster Analysen!

28 %

der Datenschutzverletzungen involvieren interne Akteure

12 %

der Datenschutzverletzungen stehen im Zusammenhang mit Rechte-Missbrauch

Data Breach Investigations Report 2018 (Verizon)

3 SICHERHEIT OPTIMIEREN

Nachdem Sie die Grundlagen der IT-Sicherheit umgesetzt haben, können Sie sich auf hochwertige Maßnahmen zur Sicherung kritischer Aspekte Ihres Unternehmens konzentrieren. Nehmen Sie sich die Ergebnisse Ihrer Risikoanalyse vor und optimieren Sie Schritt für Schritt Ihre operative Sicherheit.

3.1 ENDGERÄTESICHERHEIT STÄRKEN

ANWENDUNGEN KONTROLLIEREN

Investieren Sie in eine Anwendungskontrolle, die es Ihnen ermöglicht, alle vertrauenswürdigen Anwendungen auf eine Whitelist zu setzen und die übrigen zu blockieren. Konfigurieren Sie die Software mithilfe von Regeln, die von sachkundigen Penetrationstestern und/oder Ihren eigenen IT-Administratoren erstellt wurden.

BACKUP-PROZESS EINRICHTEN

Minimieren Sie das Malware- und Ransomware-Risiko, indem Sie einen zuverlässigen Backup-Prozess einrichten, der die betriebssystemrelevante Anwendungssoftware und sämtliche Daten abdeckt. Erstellen Sie Wiederherstellungs- und Gegenmaßnahmenpläne, die Sie quartalsweise aktualisieren und testen.

Ransomware stieg um

62 %

im Jahr 2017

The Changing State of Ransomware (F-Secure)

TIPP!

Halten Sie nach Komponenten für den Endgeräteschutz Ausschau, die Ihnen zusätzliche Erkennungsfunktionen gegen Ransomware bieten und eine leichte Überwachung und Isolation wichtiger Dateien ermöglichen.

3.2 ERKENNUNG & REAKTION

DATEN ERHEBEN

Erwerben Sie eine Erkennungs- und Reaktionslösung und sammeln, verwalten und analysieren Sie forensische Beweise. Wählen Sie basierend auf Ihrer IT-Infrastruktur und den relevantesten Bedrohungen welche Art von Beweisen Sie sammeln möchten. Passen Sie dabei Ihre Vorgehensweisen stets an die aktuelle Bedrohungslandschaft an.

KI EINSETZEN

Setzen Sie modernste Analysen ein, um Anomalien zu erkennen. Hierzu wird die Korrelation zwischen Daten und Bedrohungsanalyse-Feeds, die auf ungewöhnliche Verhaltensmuster, Abweichungen von Routinen sowie Zeichen von Tunneling-Software prüfen, genutzt. Passen Sie Ihre Analysemodelle kontinuierlich an Ihre Erfahrungen und Datenvolumina an.

MENSCHLICHES WISSEN NUTZEN

Ziehen Sie Experten hinzu, die Ihnen dabei helfen, den Überblick in Ihren Analysetools zu behalten und sich auf die wenigen Anomalien zu konzentrieren, die für Sie wirklich relevant sind. Technologien helfen Ihnen zwar dabei, Bedrohungen großflächiger zu erkennen, doch nichts ersetzt die aufmerksamen Augen eines Experten. Sie brauchen auch kompetente Fachleute, die auf Vorfälle reagieren können, sollte ein Angriff Ihre Verteidigungsmechanismen durchbrechen.

TIPP!

Ziehen Sie in Erwägung, Ihre Erkennungs- und Reaktionsaktivitäten als Managed Service (MDR; Managed Detection & Response) umzusetzen. Die Erkennung von Anomalien ist ohne die entsprechende Untersuchungs- und Reaktionsexpertise nicht sonderlich nützlich. Doch nur wenige Unternehmen besitzen diese intern.

77 %

der Angriffe auf Endgeräte im Jahr 2017 nutzten dateilose Malware und Exploits

The State of Endpoint Security Risk Report 2017 (Ponemon Institute for Barkly)

3.3 CLOUD-DIENSTE SCHÜTZEN

BESTANDSAUFNAHME DER CLOUD MACHEN

Machen Sie eine Bestandsaufnahme aller von Ihren Mitarbeitern genutzten Cloud-Dienste. Sie werden vielleicht überrascht sein, wie viele Menschen kostenlose Services als Unterstützung im Arbeitsalltag nutzen. Gehen Sie die Liste durch, identifizieren Sie die Services, die ein erhöhtes Sicherheitsrisiko darstellen könnten, und minimieren Sie Schwachstellen oder verbieten Sie deren Nutzung. Denken Sie daran: Alles in der Cloud unterliegt einer kollektiven Verantwortung.

95 %

der Cloud-Sicherheitsvorfälle werden bis 2020 auf menschliche Fehler zurückzuführen sein

Why Cloud Security Is Everyone's Business (Gartner)

CLOUD-SICHERHEIT VERBESSERN

Wenn Ihr Unternehmen stark von einem bestimmten Cloud-Dienst abhängig ist, halten Sie nach zusätzlichen Softwarelösungen Ausschau, die Ihnen eine zusätzliche Schutzebene zur Standard-Endgerätesicherheit bietet. Eine maßgeschneiderte Cloud-Schutzlösung hilft Ihnen dabei, Angriffe rechtzeitig zu stoppen, damit Ihre Daten sicher sind und Ihre Dienste unterbrechungsfrei laufen.

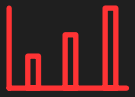
TIPP!

Achten Sie darauf, dass zusätzlich verwendete Lösungen zur Verbesserung der Sicherheit Ihrer Cloud-Dienste auch umfassende Analyse- und Reporting-Funktionen bieten. Wenn Sie bei einem möglichen späteren Sicherheitsvorfall nutzbare Daten zur Verfügung haben, ist das ein großer Vorteil!

3.4 EXPERTEN HINZUZIEHEN

SICHERHEIT PRÜFEN

Engagieren Sie Berater für eine umfassende Sicherheitsprüfung Ihrer digitalen Geschäftsstruktur, die die gesamte Software und Hardware abdeckt.



RISIKOBEURTEILUNG VERBESSERN

Halten Sie Ihre Risikobeurteilungen aktuell, indem Sie die Erkenntnisse von Experten hinsichtlich der aktuellen Bedrohungslandschaft und branchenspezifischer Probleme nutzen. Manche Berater können auch maßgeschneiderte Sicherheitsschulungen und -seminare anbieten.

ANGRIFF SIMULIEREN

Engagieren Sie ein erfahrenes Red Team, um einen hoch komplexen, mehrschichtigen Angriff auf Ihr Unternehmen zu simulieren. Setzen Sie dann auf Basis der Ergebnisse entsprechende Verbesserungen um. Das sollte Ihre größten Sicherheitslücken schließen.

68 %

der Datenschutzverletzungen dauerten Monate oder länger, bis sie erkannt wurden

Data Breach Investigations Report 2018 (Verizon)

TIPP!

Wenn Sie eine Red-Team-Übung noch intensivieren möchten, geben Sie den Penetrationstestern die Erlaubnis, in Ihr Bürogebäude einzubrechen. Wussten Sie, dass Sie einen Fingerabdruckscanner mithilfe von Toilettenpapier umgehen können?

SEIEN SIE KEIN LEICHTES ZIEL

Die meisten erfolgreichen Cyber-Angriffe sind nicht sonderlich komplex. Sie werden mit vorgefertigten Exploits von einfachen Cyber-Kriminellen durchgeführt, die die gängigen technologischen und verhaltensbezogenen Schwachstellen ausnutzen. Unser bester Rat an Sie ist daher einfach: Machen Sie sich nicht selbst zur Zielscheibe.

Dank 30 Jahren Branchenerfahrung kennen wir uns mit Cyber-Sicherheit aus. Hier können Sie sich unsere umfassenden Cloud- und Vor-Ort-Cyber-Sicherheitslösungen für Unternehmen ansehen.

Obwohl eigentlich eher gängige Bedrohungen nach Schema F das größte Risiko darstellen, steigt in der aktuellen Bedrohungslandschaft für alle Unternehmen die Wahrscheinlichkeit, auch Opfer komplexer Angriffe zu werden. F-Secure verfügt über langjährige Erfahrung mit der Bereitstellung von Sicherheitslösungen für Unternehmen in den Bereichen Gesundheitswesen, Technologie und Produktion sowie in anderen Branchen, die häufig Ziel von Angriffen sind. Aber auch für nationale Verteidigungsorganisationen sind wir tätig. Wir wissen, wie sich selbst die komplexesten Cyber-Angriffe bekämpfen lassen.

FÜR ALLE UNTERNEHMEN STEIGT DIE WAHRSCHEINLICHKEIT VON KOMPLEXEN ANGRIFFEN

Entdecken Sie hier unsere modernen Cyber-Sicherheitslösungen für Unternehmen. Sie können bei uns auch eine Beurteilung Ihrer Sicherheitsumgebung, Schwachstellen oder Risiken anfragen.

GANZHEITLICHE CYBER-SICHERHEIT

Die einzige Möglichkeit, Ihr Unternehmen wirklich zu schützen, ist ein ganzheitlicher Sicherheitsansatz. Eine einfache Bedrohungsprävention ist nicht mehr ausreichend. Angreifern immer einen Schritt voraus zu sein, erfordert Vorbereitung, Aufmerksamkeit und Einsatz.

Und die richtigen Technologien. Ein stabiler Cyber-Sicherheitsplan auf Basis einer einzigen Lösung ist vielleicht nicht möglich, aber auch das andere Extrem ist unnötig. Alles, was Sie brauchen, um Ihre Sicherheit von einem passablen auf ein ausgezeichnetes Niveau zu bringen, sind ein paar sorgfältig ausgewählte Produkte und Services.

Wenn Sie mehr über ganzheitliche Cyber-Sicherheit wissen möchten, kontaktieren Sie uns und sprechen Sie mit einem unserer Experten.

ÜBER F-SECURE

Niemand kennt sich mit Cyber-Sicherheit besser aus als F-Secure.

Bereits seit drei Jahrzehnten setzt sich F-Secure für Innovationen in der Cyber-Sicherheit ein und schützt Zehntausende von Unternehmen und Millionen von Menschen vor Angriffen. Mit beispielloser Erfahrung im Endgeräteschutz sowie mit Erkennungs- und Reaktionsvorgängen schirmt F-Secure Unternehmen und Verbraucher gegen alles ab – komplexe Cyber-Angriffe und Verletzungen der Datensicherheit genauso wie ausgedehnte Ransomware-Infektionen.

Die hochentwickelte Technologie von F-Secure verbindet die Leistungsfähigkeit des maschinellen Lernens mit der Kompetenz des Fachpersonals in seinen weltweit anerkannten Sicherheitslaboren zu einem einzigartigen Ansatz mit dem Namen Live Security. Mit seinen Sicherheitsexperten war F-Secure an mehr europäischen Untersuchungen zu Cyber-Kriminalität beteiligt als jedes andere Unternehmen am Markt. Unsere Produkte werden weltweit durch über 200 Breitband- und Mobilfunkbetreiber sowie zahlreiche Reseller vertrieben.

F-Secure wurde 1988 gegründet und ist an der Börse NASDAQ OMX Helsinki Ltd. notiert.

www.f-secure.com
blog.f-secure.com
www.twitter.com/fsecure
www.facebook.com/f-secure

F-Secure