

Bedrohungsprognosen für 2018

McAfee Labs

Machine Learning

Die Entwicklungen bei Machine Learning-Technologien zum Schutz von Unternehmen werden das Wettrennen zwischen Verteidigern und Angreifern weiter befeuern.



Cyber-Kriminelle

Cyber-Kriminelle setzen für ihre Angriffe ebenfalls Machine Learning ein.



Erkennung und Behebung

Machine Learning erkennt und behebt Schwachstellen, verdächtiges Verhalten sowie Zero-Day-Angriffe.



Schnellere Entscheidungen

Die Zusammenarbeit von Mensch und Maschine verändert unsere Einschätzungen und beschleunigt Entscheidungen.

Ransomware

Die Rentabilität herkömmlicher Ransomware-Angriffe geht in Anbetracht immer besserer Abwehrmaßnahmen zurück, und der Schwerpunkt der Angreifer verlagert sich auf finanziell lohnenswerte Personen, Sabotage und Geschäftsunterbrechungen.

Die Zahl der Ransomware-Varianten stieg in den letzten vier Quartalen insgesamt um 56 %.



Weniger Varianten

Die Zahl der Ransomware-Varianten geht zurück, da die Angreifer auf dem Schwarzmarkt vorgefertigte Produkte kaufen.



Stoppen von Zahlungen

NoMoreRansom.org unterstützt Opfer beim Stoppen von Zahlungen.



Mehr Angriffe

Es gibt immer mehr Angriffe durch skrupellose Mitbewerber oder Kriminelle, die auf Schutzgelderpressung abzielen.



Stoppen von Cyber-Kriminellen

Die Cyber Threat Alliance unterstützt Strafverfolgungsbehörden beim Stoppen von Cyber-Kriminellen.

Server-lose Apps

Server-lose Apps können Zeit sparen und Kosten reduzieren, aber auch die Angriffsfläche vergrößern.



Übertragene Daten

Die Daten sind bei der Übertragung im Netzwerk gefährdet.



Individuellere Bearbeitung

Ermöglicht individuellere Bearbeitung und dadurch z. B. schnellere Abrechnung.



Rechteeskalationen und Anwendungsabhängigkeiten

Es besteht das Risiko von Rechteeskalationen und Anwendungsabhängigkeiten.

Eingriff in die Privatsphäre

Hersteller, die ihre Einnahmen steigern wollen, erfassen unsere persönlichen Daten – mit und ohne unsere Zustimmung.



Unternehmen

Unternehmen könnten gegen Gesetze verstoßen, die Strafe zahlen und wie bisher weitermachen.



Verträge

Verbraucher lesen Verträge nur selten, und Unternehmen ändern sie häufig nachträglich.



Vernetzte Geräte

Vernetzte Geräte übertragen zu viele Informationen.

Schutz für Ihre Kinder

Unsere Kinder sehen einer erstaunlichen Zukunft mit zahlreichen Geräten, Diensten und Erlebnissen entgegen – aber auch einer Zukunft voller erheblicher Risiken für ihre Privatsphäre.



Online-Historie

Die Online-Historie – Videos oder Fotos in Bars – kann zu digitalem Ballast werden.

Arbeitgeber

Die Einstellungsentscheidungen der Arbeitgeber werden von Suchergebnissen beeinflusst.

Ändern von Standardkennwörtern

Deaktivieren Sie nicht benötigte Funktionen, und ändern Sie Standardkennwörter.

Bedrohungsprognosen von McAfee Labs für 2018

Den vollständigen Report finden Sie unter www.mcafee.com/2018Predictions.